

Speaking Up or Staying Silent – Corporate Accountability, Procurement and the Supply Chain



Procurement and Supply Chain Management Made Simple.

Subject	Page
<i>Foreword</i>	5
<i>Whistleblowing as a Governance Control</i>	6
<i>Why Boards Should Care</i>	6
<i>The Board's Responsibility</i>	7
<i>Audit and Risk Committees</i>	7
<i>Internal Audit and Whistleblowing</i>	8
<i>Executive Management</i>	8
<i>HR, Legal, Compliance and Internal Audit – Who Owns Whistleblowing?</i>	9
<i>Conflicts at the Top</i>	9
<i>Independent Oversight</i>	10
<i>Reporting Whistleblowing Data to the Board</i>	11
<i>Why Zero Reports May Be a Warning Sign</i>	11
<i>High Reporting Levels Are Not Necessarily Bad</i>	12
<i>Substantiation Rates</i>	12
<i>Repeat Concerns</i>	13
<i>Learning from Disclosures</i>	13
<i>Whistleblowing and Organisational Risk Registers</i>	14
<i>Why Procurement Is Particularly Exposed</i>	14
<i>Commercial Pressure and Ethical Pressure</i>	15
<i>Supplier Dependence</i>	16
<i>Procurement's Unique Visibility</i>	16
<i>Supplier Bribery</i>	17
<i>Bribes Disguised as Legitimate Commercial Activity</i>	17
<i>Gifts and Hospitality</i>	18
<i>Travel, Entertainment and Supplier Hospitality</i>	18
<i>Third-Party Intermediaries</i>	19
<i>Whistleblowing as Anti-Bribery Intelligence</i>	19
<i>Conflicts of Interest</i>	20
<i>Undisclosed Supplier Relationships</i>	21
<i>Supplier Favouritism</i>	22
<i>Repeated Awards</i>	22
<i>Declarations of Interest</i>	23
<i>Speaking Up About Senior Conflicts</i>	23
<i>Tender Manipulation</i>	24
<i>Leaking Tender Information</i>	24
<i>Manipulating Evaluation Scores</i>	25
<i>Bid Rigging and Collusion</i>	25
<i>Artificial Competition</i>	26
<i>Warning Signs Procurement Teams May See First</i>	27

Subject	Page
<i>Why Whistleblowing Complements Competition Controls</i>	27
<i>Invoice Fraud</i>	28
<i>Phantom Services</i>	28
<i>Purchase Order Manipulation</i>	29
<i>Splitting Expenditure</i>	29
<i>Retrospective Purchase Orders</i>	30
<i>Supplier Bank-Account Changes</i>	31
<i>Fraudulent Supplier Creation</i>	31
<i>Employee-Controlled Suppliers</i>	32
<i>Tender Confidentiality</i>	32
<i>Information Leaks</i>	33
<i>Using Insider Information to Advantage a Supplier</i>	34
<i>Data Access and Audit Trails</i>	34
<i>Beyond the Immediate Supplier</i>	35
<i>Modern Slavery and Labour Exploitation</i>	35
<i>Human-Rights Abuses Below Tier One</i>	36
<i>Recruitment Fees and Debt Bondage</i>	36
<i>Child Labour and Forced Labour</i>	37
<i>Migrant Workers and Vulnerability</i>	38
<i>Health-and-Safety Failures</i>	38
<i>Product Safety and Quality Manipulation</i>	39
<i>Counterfeit Components</i>	39
<i>Falsified Testing</i>	40
<i>Suppressed Non-Conformities</i>	40
<i>Whistleblowing Before the Recall</i>	41
<i>Environmental Misconduct</i>	42
<i>False Sustainability Claims</i>	42
<i>Greenwashing Inside the Supply Chain</i>	43
<i>Carbon and Environmental Data Manipulation</i>	43
<i>Whistleblowing and ESG Assurance</i>	44
<i>Falsification of Supplier Performance Data</i>	45
<i>False Certifications and Audit Evidence</i>	45
<i>Social Audit Manipulation</i>	45
<i>Gaming Service-Level Agreements</i>	46
<i>Whistleblowing as a Counterweight to Self-Reporting</i>	47
<i>Cybersecurity Failures</i>	47
<i>Concealed Data Breaches</i>	48
<i>Inappropriate System Access</i>	49
<i>Third-Party Cyber Risk</i>	49

Subject	Page
<i>Reporting Technology Misuse</i>	50
<i>The Supplier's Employees as a Source of Assurance</i>	50
<i>Should Buyers Provide External Speak-Up Channels?</i>	51
<i>Protecting Supplier Whistleblowers</i>	52
<i>Supplier Codes of Conduct</i>	52
<i>Building Speak-Up Obligations into Contracts</i>	53
<i>Supplier Notification Duties</i>	53
<i>Pass-Through Requirements</i>	54
<i>Audit Rights</i>	55
<i>Non-Retaliation Commitments</i>	55
<i>Serious Breach and Remediation</i>	56
<i>Digital Whistleblowing Platforms</i>	56
<i>Artificial Intelligence and Whistleblowing</i>	57
<i>AI as a New Source of Risk</i>	57
<i>Data Analytics as the Second Whistleblower</i>	58
<i>Procurement Analytics</i>	59
<i>Protecting Whistleblower Data</i>	59
<i>Can Technology Identify an Anonymous Reporter Accidentally?</i>	60
<i>Different Legal Regimes</i>	60
<i>Cultural Differences</i>	61
<i>Whistleblowing and the Global Supply Chain</i>	62
<i>Workers Where Legal Protection Is Weak</i>	62
<i>Cross-Border Investigations</i>	63
<i>Global Standards with Local Delivery</i>	64
<i>Procurement Professionals as Both Gatekeepers and Whistleblowers</i>	64
<i>Create Escalation Routes Outside the Procurement Hierarchy</i>	65
<i>Build Whistleblowing into Supplier Governance</i>	65
<i>Protect Procurement Integrity</i>	66
<i>The Buyer's Responsibility Does Not End at Tier One</i>	66
<i>Speaking Up or Staying Silent?</i>	67
<i>Can Legislation Create Courage?</i>	68
<i>Can Governance Reduce the Need for Courage?</i>	68
<i>When Commercial Success Conflicts with Speaking Up</i>	69
<i>The Cost of Ignoring the Messenger</i>	69
<i>Summary – Silence Is a Governance Decision Too</i>	69
<i>Further Reading</i>	70

Foreword

Whistleblowing is more than an employment safeguard or legal reporting route; it is a source of organisational intelligence. Boards, audit committees and procurement professionals cannot manage risks they do not know about, and formal reporting systems inevitably reveal only part of operational reality. The Financial Reporting Council describes effective speak-up arrangements as an early-warning system that helps organisations manage risk, placing employee voice firmly within the wider architecture of governance and internal control.

The value of that intelligence is visible in regulatory data. During 2025–26, the Financial Conduct Authority assessed 1,375 whistleblowing reports containing 4,375 allegations, with the information contributing to 523 instances of direct action. A further 53% of closed cases informed wider regulatory work and harm prevention. Those figures show that disclosures can remain useful even when they do not produce immediate enforcement, because they reveal patterns, vulnerabilities, and emerging risks.

For procurement and supply chains, the argument is particularly compelling. UK public bodies spent an estimated £407 billion procuring goods and services in 2023–24, around one third of public-sector expenditure. Behind those transactions sit suppliers, subcontractors, workers, advisers and systems that conventional assurance cannot observe continuously. People closest to operations may see bribery, fraud, exploitation, unsafe products, cyber weaknesses or manipulated performance data long before those problems appear in formal dashboards.

The challenge for leadership is therefore not simply to create a channel, but to ensure that information can travel safely from the person who sees the warning sign to those capable of acting upon it. Whistleblowing should sit alongside audit, analytics, risk management and supplier assurance, testing the official account against lived operational reality. Organisations become more governable when they treat uncomfortable information not as disloyalty, but as intelligence they cannot afford to lose.

Whistleblowing as a Governance Control

Whistleblowing should sit beside enterprise risk management, internal control, compliance monitoring and assurance as a formal source of governance intelligence. The FRC's 2024 UK Corporate Governance Code requires applicable boards to provide confidential, if desired anonymous, routes for concerns, routinely review the arrangements and resulting reports, and ensure proportionate, independent investigation and follow-up. Speak-up data therefore belongs within the control environment, not in an isolated employee-relations file.

Regulators already treat such information as actionable intelligence rather than an isolated grievance. Disclosures are triaged, matched against existing supervisory data and, where warranted, escalated into formal investigation or enforcement referral, converting individual accounts into institutional knowledge. Any single allegation may remain unsubstantiated even where the underlying pattern is genuine, because verification takes time and evidence is often incomplete. Boards should therefore treat reporting channels as sensors that reveal patterns, not scoreboards measuring individual case outcomes.

Carillion illustrates the cost of weak challenge across governance and assurance. Before its January 2018 liquidation, it held around 420 UK public-sector contracts; Parliament recorded nearly £7 billion of liabilities and only £29 million of cash. Deloitte, its internal auditor, had been paid more than £10 million, yet only 15 of 309 recommendations between 2012 and 2016 were rated high priority. A control system can exist extensively on paper and still fail to surface danger.

Why Boards Should Care

Boards should care because management information is inevitably filtered through organisational structures, incentives and judgement. Dashboards normally report what has been measured, escalated and classified; whistleblowers can reveal what has been suppressed, normalised or never recorded. A polished risk register may therefore coexist with serious misconduct on the ground. The governance question is not whether every allegation is correct, but whether decision-makers can hear credible dissent before losses, prosecutions or public harm make it unavoidable.

Tesco provides a striking private-sector example involving supplier income. In September 2014, concerns about how it recognised commercial income reached senior leadership and triggered an independent investigation. The later judicial record put the relevant profit overstatement at £284 million. Tesco Stores subsequently entered a deferred prosecution agreement carrying a £128,992,500 financial penalty and £3 million towards investigation costs. The lesson is governance-specific: information from inside the operating model can contradict apparently authoritative financial reporting.

The Post Office Horizon scandal shows the scale of the problem when warnings, system evidence, contractual relationships, and governance become disconnected. The statutory inquiry has examined governance, Horizon monitoring, contractual arrangements, internal and external audit, oversight and whistleblowing. By 28 August 2026, government data showed approximately £1.697 billion had been paid in financial redress. That figure does not measure every cost, but illustrates why boards must interrogate persistent challenge rather than treat it as organisational noise.

Regulatory data reinforces the point. In April to June 2026, the FCA received 333 whistleblowing reports containing 886 allegations. Of 395 reports closed, 14% resulted in significant action to manage harm, 29% in action to reduce harm and 49% informed wider work, including harm prevention, without direct action. Boards should not expect every disclosure to become a proven case; intelligence can still improve supervision, controls and future decisions.

For procurement and supply-chain governance, the practical test is whether speak-up intelligence changes decisions. Boards should expect significant allegations to be cross-

checked against supplier performance, contract variations, rebates, pricing anomalies, conflicts declarations, audit findings, quality failures, safety incidents and payment data. Repeated reports concerning one category, executive sponsor, intermediary or supplier deserve pattern analysis. Management reporting explains the organisation through authorised channels; whistleblowing can reveal the parts of that explanation that are incomplete.

The Board's Responsibility

Board responsibility must be described accurately because UK requirements differ by sector and legal form. For companies applying the 2024 UK Corporate Governance Code, Provision 6 places clear expectations on the board to review speak-up arrangements and reports. In specified FCA-regulated businesses, whistleblowing systems form part of risk management, and an effectiveness report must reach the governing body at least annually. Other organisations may face different statutory, regulatory, contractual or governance frameworks.

Whistleblowing protection sits in Part IVA of the Employment Rights Act 1996, inserted by the Public Interest Disclosure Act 1998, rather than a universal duty for identical board schemes. Since 1 September 2025, the failure-to-prevent-fraud offence can expose an organisation meeting at least two thresholds—more than 250 employees, over £36 million turnover and over £18 million assets—to an unlimited fine where an associated person commits fraud for its benefit and reasonable prevention procedures were absent.

Culture is a board-level control question, not an employee-engagement slogan. The 2024 Civil Service People Survey found that, among respondents who did not report bullying or harassment, 64% doubted corrective action would follow, 46% feared being seen as troublemakers and 41% feared jeopardising their jobs. Those figures are not whistleblowing statistics, but they reveal the behavioural conditions that can suppress challenge. Boards should test whether comparable fears exist within their own workforce and supply chain.

Audit and Risk Committees

Audit and risk committees are suited to examining whistleblowing without becoming substitute investigators. Their role should be to test whether concerns are classified properly, investigated independently, resolved and translated into control improvements. Where the board delegates detailed oversight, responsibility does not disappear: the committee should report material themes, unresolved cases and systemic weaknesses back to the board. It should also challenge whether management has downgraded, fragmented or repeatedly closed related concerns without recognising a pattern.

Good oversight requires more than counting cases. Committees should examine ageing, severity, substantiation, business area, supplier involvement, investigation quality, remediation, recurrence and allegations of retaliation. The FRC encourages boards to record the number and type of incidents raised, actioned and closed, together with lessons learned. In procurement, that dataset should link to tender complaints, conflicts, single-source awards, contract changes, payment exceptions, quality failures and supplier assurance so separate signals can be analysed together.

Regulatory outcomes demonstrate why committees should avoid judging a channel solely by enforcement results. England's Regulator of Social Housing concluded 22 qualifying disclosures in 2025–26; 21 received detailed consideration, and all 21 were investigated, yet none directly produced published regulatory action. In 15 cases, the regulator obtained assurance that providers were responding appropriately, while in six cases it informed ongoing regulatory intelligence. Testing, assurance and intelligence can therefore be valuable outcomes even when formal sanctions do not follow.

Consistently favourable assurance ratings deserve particular scrutiny, not automatic reassurance. Collapsed organisations have sometimes shown internal-audit programmes rating the great majority of reviews satisfactory shortly before problems proved existential. An audit or risk committee should therefore ask whether assurance ratings reflect operational

reality, whether scope excludes difficult areas, and whether dissenting evidence from employees, subcontractors or suppliers contradicts formal reports. Comfortable assurance should trigger curiosity, not reassurance, when operational intelligence points elsewhere.

Internal Audit and Whistleblowing

Internal audit should treat whistleblowing as a source of risk intelligence, not merely another process to inspect periodically. Disclosures can identify controls that appear satisfactory in policy but fail in practice, particularly where management override, local custom or supplier relationships distort formal procedures. Risk-based audit planning should consider speak-up themes alongside incidents, complaints, contract performance and regulatory intelligence. A recurring allegation may justify targeted assurance even where no individual case has yet been substantiated.

The relationship must preserve independence. Internal audit can review the design and effectiveness of whistleblowing arrangements, test investigation governance, examine whether remediation was completed and use themes to shape the audit universe. It should be cautious about owning the reporting channel or routinely investigating allegations it will later assure over the same system. Where internal audit undertakes investigative work, safeguards, reporting lines and subsequent independent review should prevent self-review from weakening confidence.

Procurement creates particularly rich opportunities for triangulation. Internal auditors can compare disclosures with purchase-order overrides, tender-scoring changes, unusually concentrated awards, retrospective approvals, contract variations, duplicate invoices, supplier master-data amendments, rebates, gifts, hospitality, and conflicts declarations. Given the sheer scale of UK procurement expenditure, even small control weaknesses can compound quickly across thousands of transactions. Speak-up themes should therefore influence both transaction testing and strategic reviews of category and supplier governance.

External intelligence can strengthen that planning. The Competition and Markets Authority offers rewards of up to £250,000 for information about cartels, while businesses involved in cartel conduct can face civil penalties of up to 10% of turnover; individuals may face up to five years' imprisonment. Procurement auditors should understand bid-rigging indicators and escalation routes. A confidential allegation about coordinated bids, cover pricing or market sharing may be an internal-control issue and evidence requiring legal handling.

The strongest feedback loop is measurable: a concern identifies a possible weakness; investigation establishes facts; management implements remediation; internal audit tests whether the control now works; and the audit committee monitors recurrence. That cycle converts whistleblowing from reactive case management into organisational learning. It also prevents a common governance failure in which cases are marked closed. At the same time, the underlying incentive, supplier dependency, approval weakness or leadership behaviour remains untouched and generates the next disclosure.

Executive Management

Executive management determines whether board policy survives contact with daily reality. Senior leaders set incentives, allocate investigators, control information flows and decide whether managers are rewarded for surfacing problems or for keeping dashboards green. They should make clear that raising a concern will not damage careers, require prompt preservation of evidence, stop suspected misconduct where necessary and ensure remediation has named owners and deadlines. Tone matters, but operational consequences determine whether employees believe it.

Public contracting provides costly examples of what happens when control failures reach commercial relationships. Serco Geografix's deferred prosecution agreement required a £19.2 million payment to the Serious Fraud Office after conduct connected with electronic-monitoring contracts; Serco had also compensated the Ministry of Justice by £70 million. G4S Care and

Justice Services later agreed to a £38.5 million penalty, alongside a £121.3 million civil settlement. Both cases were accompanied by significant compliance, assurance and management remediation.

The failure-to-prevent-fraud offence sharpens executive accountability for prevention. Since September 2025, qualifying large organisations can be criminally liable where an employee, agent, subsidiary undertaking or associated person commits specified fraud intending to benefit the organisation and reasonable prevention procedures were absent; directors need not have known about it. Executive management must therefore link speak-up arrangements to fraud risk assessment, due diligence, contract controls, training, incentives, monitoring, and escalation, rather than treating them as separate programmes.

HR, Legal, Compliance and Internal Audit – Who Owns Whistleblowing?

Whistleblowing is safest when accountability is clear, but ownership is distributed. The board should retain oversight; an appropriately independent senior sponsor should protect the system's integrity; operational handling can then draw on HR, legal, compliance, security, procurement, finance, or internal audit, depending on the allegation. No single function sees every risk dimension. A concern about a supplier rebate, for example, may involve employment retaliation, fraud, accounting, conflicts, contract rights and regulatory reporting simultaneously.

HR brings expertise in employee relations, disciplinary processes and protection against detriment, but a disclosure should not be reduced to a grievance. Legal advisers can preserve privilege where it applies, identify reporting duties and protect due process, yet excessive legalisation can make the system appear defensive. Compliance understands regulatory obligations and misconduct typologies. Internal audit can test controls and themes. Procurement contributes commercial evidence, supplier records and category knowledge that other functions may not possess.

Concentrating the entire process within one function creates blind spots. HR may focus on interpersonal conduct when the underlying issue is fraud; legal teams may understandably prioritise litigation risk; compliance may confine analysis to regulated breaches; internal audit may compromise later assurance if it owns investigations it must subsequently review. A multidisciplinary triage model reduces these risks, provided confidentiality remains controlled and the whistleblower is not repeatedly required to retell sensitive information to different teams.

Financial-services regulation provides a useful governance model. FCA rules require relevant organisations to appoint a whistleblowers' champion responsible for the integrity, independence, and effectiveness of arrangements, including protection against victimisation. The FCA expects that role to sit with a non-executive director, while making clear that the champion need not handle disclosures daily. Separating oversight from operational processing helps because independence weakens when the same people receive, investigate, defend, and assure the case.

Tesco's 2014 accounting crisis shows the value of escalation beyond the management chain. Reporting recorded that a whistleblower took concerns about supplier-related commercial income to the general counsel, after which leadership commissioned an independent investigation. The resulting scrutiny exposed an overstatement and led to regulatory and criminal consequences. The governance lesson is not that legal should own whistleblowing, but that credible concerns need alternative routes that can bypass levels where resistance or conflict may exist.

Conflicts at the Top

The most difficult disclosures implicate chief executives, finance directors, board chairs, or other people who control ordinary escalation routes. A whistleblowing framework is structurally weak if every serious concern ultimately returns to the person named in it. Policies should

therefore specify bypass routes to the audit chair, senior independent director, another designated non-executive or an external channel, with authority to secure records, commission advice and protect the reporting person from interference or retaliation.

The UK Corporate Governance Code reinforces that principle. Provision 7 requires boards to identify and manage conflicts of interest and ensure third-party influence does not override independent judgement. Provision 8 states that unresolved director concerns about board operation or company management should be recorded in board minutes, and resigning non-executives should provide a written statement where appropriate. These mechanisms are broader than whistleblowing, but they support the same proposition: serious challenge must not disappear inside hierarchy.

FCA rules offer a more specific model for regulated organisations. The whistleblowers' champion must oversee the integrity, independence and effectiveness of whistleblowing policies and should have sufficient authority, resources, information and access to independent legal advice. That architecture is useful beyond financial services. Where an allegation concerns executive management, the receiving route, investigator, scope approval and final decision-maker should all be sufficiently independent of the subject to withstand later regulatory, judicial or public scrutiny.

The Post Office Horizon Inquiry demonstrates why escalation design deserves board attention before a crisis. Its phases on governance and whistleblowing have examined executive leadership, board oversight, contractual arrangements, technical competence, internal and external audit and the handling of challenges over many years. The inquiry's existence should not be used to pre-judge individual liability, but the governance lesson is already clear: a route that cannot safely challenge senior authority is not a reliable control.

Independent Oversight

Independent oversight is most valuable where the organisation's normal incentives may favour silence. Non-executive directors and audit chairs can ask questions without owning operational targets, supplier relationships or management bonuses, giving them a different vantage point from executives. Their role is not to assume every allegation is true, but to ensure serious concerns receive fair triage, competent investigation and proportionate action. Independence means freedom from the interests being examined, not distance from accountability.

The FCA's whistleblowers' champion model illustrates the principle. Relevant regulated organisations must give the champion responsibility for the integrity, independence and effectiveness of whistleblowing arrangements, and the regulator expects a non-executive director to hold the role where practicable. The champion should have sufficient authority, resources, information and access to independent legal advice. That combination matters because nominal independence is ineffective if the oversight role cannot obtain evidence, challenge executives or commission specialist support when necessary.

Independent advisers can be valuable where allegations concern directors, complex accounting, bribery, procurement fraud, competition law or disputed products. Their appointment should not become an automatic reflex or a way to shift responsibility. The board or committee commissioning the work should define scope, preserve evidence, manage conflicts, require factual reporting and track remediation. Where external investigators depend financially on management for continuing instructions, governance safeguards should ensure uncomfortable findings cannot be narrowed, delayed or buried.

External reporting routes also matter when internal independence is doubtful. In 2025–26, the Charity Commission received 594 whistleblowing reports, up from 547 the previous year. The Serious Fraud Office managed 167 qualifying disclosures in 2024–25 and acted in more than 92% of them. Prescribed-person channels cannot replace healthy internal governance, but their use shows why organisations should assume unresolved concerns may eventually reach regulators, accompanied by records, documents, or other evidence accumulated outside

management reporting.

For procurement and supply chains, independent escalation can extend beyond employment concerns. The CMA offers up to £250,000 for useful cartel information because price-fixing, market-sharing and bid-rigging are deliberately concealed. Businesses found participating can face penalties up to 10% of turnover, while individuals may face imprisonment for up to five years. Audit chairs and non-executives should recognise that a supplier or tender allegation can carry competition, fraud and public-procurement implications far beyond a conduct complaint.

Reporting Whistleblowing Data to the Board

Board reporting should turn individual cases into decision-useful intelligence without unnecessarily exposing identities. A mature dashboard tracks volume, reporting route, allegation category, business area, supplier or third-party involvement, severity, ageing, investigation duration, outcome, substantiation, remediation and recurrence. It should separately record alleged retaliation and whether reporters would speak up again. FCA rules require relevant organisations to report at least annually on whistleblowing-system effectiveness while maintaining individual confidentiality; stronger governance normally requires more frequent thematic reporting.

NHS data illustrates the value of analysing themes rather than volume. Freedom to Speak Up Guardians recorded 37,770 cases in 2025–26. Worker safety or wellbeing featured in 15,367 cases (41% of the total), while bullying or harassment featured in 17%. More than 1,100 cases, around 3%, included reported detriment after speaking up, while 76% of respondents said they would speak up again. Boards need both usage and retaliation indicators because volume alone cannot establish psychological safety.

Numbers require interpretation. Rising reports may indicate deteriorating conduct, greater trust in the channel, better awareness or several effects at once; zero reports can indicate either low misconduct or a culture too unsafe to speak. Boards should therefore compare trends with workforce surveys, audit findings, fraud losses, supplier complaints, regulatory contact and operational incidents. The most important measures are whether concerns are heard early, investigated well, resolved fairly, followed by remediation and prevented from recurring.

Why Zero Reports May Be a Warning Sign

A complete absence of whistleblowing reports can look reassuring, yet in a sizeable organisation it should provoke questions rather than congratulations. Wrongdoing, mistakes, conflicts and unsafe practices do not disappear simply because a reporting channel remains unused. Silence may reflect confidence that nothing serious is happening, but it can also indicate fear, ignorance of the process, distrust of confidentiality, or a belief that management will not act when concerns are raised.

UK data provides useful context. NHS Freedom to Speak Up Guardians recorded 37,770 cases in 2025–26, taking the cumulative total since the National Guardian's Office was established beyond 200,000. The FCA received 1,375 whistleblowing reports in the same financial year, while the Charity Commission received 594. These sectors differ substantially, but the volumes demonstrate that functioning reporting environments normally generate concerns rather than perfect silence across large, complex workforces.

Boards should therefore investigate unexplained silence through workforce surveys, exit interviews, grievance patterns, sickness data, supplier complaints and independent assurance. A zero-report dashboard may conceal problems that employees are taking elsewhere. External regulators provide alternative routes within their remits precisely because internal confidence can fail: the FCA, Charity Commission and Regulator of Social Housing all receive whistleblowing disclosures. Where legally possible, compare low internal reporting with external complaints and regulatory contact.

The warning is behavioural rather than mathematical. No statute requires an organisation to receive a particular number of disclosures, and a small, low-risk employer may genuinely record none. The stronger indicator is inconsistency: significant incidents, control failures or cultural survey concerns combined with no speak-up activity. Governance should ask whether people know the channel, trust confidentiality, understand protection against detriment and have seen previous concerns handled fairly, promptly and visibly enough to justify confidence.

High Reporting Levels Are Not Necessarily Bad

High reporting levels are not necessarily evidence of a troubled organisation. They may show that employees know where to go, believe confidentiality will be respected and expect concerns to be considered seriously. Mature governance therefore avoids setting targets to reduce whistleblowing numbers. Such targets can create precisely the wrong incentive, encouraging managers to discourage reports, reclassify them as grievances or resolve them informally before patterns become visible to those responsible for oversight.

The FCA offers a useful contemporary example. It assessed 1,375 whistleblowing reports in 2025–26, 22% more than in the previous year, and described the increase as demonstrating continued public trust in reporting to the regulator. Sixty-eight per cent of whistleblowers provided contact details, enabling follow-up while relying on the FCA to protect their identities. High volume, paired with a willingness to remain contactable, can therefore indicate confidence rather than organisational deterioration.

Healthcare data makes the same point from a different setting. Freedom to Speak Up Guardians received 37,770 cases during 2025–26; 12% were raised anonymously and more than 1,100 included reported detriment after speaking up. Importantly, 76% of respondents said they would speak up again. The combination matters: volume shows use, while willingness to return to the process better indicates trust than a simple year-on-year reduction in case numbers.

A rising caseload can also result from better communication, newly appointed guardians, mergers, regulatory attention or the opening of channels to contractors and suppliers. Boards should resist simplistic red-amber-green thresholds based solely on volume. More meaningful questions concern severity, source, repeat themes, retaliation, investigation quality and remediation. An increase in minor concerns raised early may be healthier than a quiet system in which only catastrophic failures eventually become visible through litigation, regulators or the media.

For procurement teams, a healthy flow of concerns can be particularly valuable because commercial misconduct is often concealed within apparently legitimate transactions. Suspicious tender similarities, unexplained specification changes, gifts, conflicts, unusual rebates or pressure to approve invoices may first appear as isolated observations. Encouraging early challenge creates a wider detection network around procurement. The objective is not a low number of reports; it is earlier visibility, proportionate investigation and fewer unresolved control failures.

Substantiation Rates

Substantiation rate is useful, but only when its definition is clear. Some organisations count a case as substantiated only where every allegation is proved; others record partial substantiation, control weakness, insufficient evidence or regulatory intelligence separately. Comparisons can therefore mislead. A low rate may reflect malicious or mistaken reports, but it may also stem from poor records, delayed escalation, inaccessible witnesses, or allegations about conduct that is difficult to prove after the event.

The Regulator of Social Housing demonstrates why outcome data needs context. In 2025–26, it processed 22 qualifying disclosures, referred 21 for detailed consideration and investigated all 21. None directly resulted in published regulatory action. Yet 15 investigations produced assurance that providers were addressing the issues appropriately, while the remaining six

informed continuing regulatory intelligence. Treating the formal enforcement figure of zero as evidence that the disclosures lacked value would therefore be plainly wrong.

Boards should examine substantiation alongside evidential quality, investigation times, repeat allegations and control improvements. An unsubstantiated allegation can still reveal a weak approval process, unclear policy, inadequate segregation of duties or poor record-keeping. Conversely, a very high substantiation rate may suggest that employees report only when evidence is overwhelming because they fear the consequences of being wrong. The healthiest system encourages reasonable concerns while carefully distinguishing between suspicion, evidence, findings, and proven misconduct.

Repeat Concerns

Repeat concerns matter because recurrence can turn an isolated allegation into evidence of a systemic weakness. Names, locations or transactions may change while the underlying control failure remains constant: poor segregation of duties, excessive management override, weak contract monitoring, conflicts, retaliation or unreliable data. Boards should therefore track themes across cases rather than close each disclosure as a self-contained event. Recurrence is often the clearest indication that remediation has treated symptoms rather than causes.

The Post Office Horizon scandal demonstrates the danger of repeatedly interpreting similar concerns as individual failures. Over many years, sub-postmasters challenged accounting discrepancies and Horizon's reliability while prosecutions and recovery action continued. The statutory inquiry has examined governance, technical assurance, audit, contractual arrangements and whistleblowing precisely because recurring complaints can expose weaknesses extending beyond any single case. Repetition should increase curiosity and scrutiny, not encourage an assumption that complainants share the same misunderstanding.

Patterns may also repeat across suppliers. The CMA's September 2026 work on bid-rigging stresses that individual contracting authorities may see professionally prepared bids without recognising connections that become visible only across tenders, organisations and time. In 2023, ten construction businesses were fined almost £60 million for colluding over demolition and asbestos-removal contracts worth approximately £150 million. Evidence included emails, messages and handwritten records showing compensation arrangements linked to manipulated bids.

A governance response is to establish recurrence triggers. Two similar allegations need not prove anything, but they may justify wider sampling, independent review or analysis of historic transactions. Procurement data can be revealing when repeated concerns are compared with award concentration, bid patterns, contract variations and approval overrides. The objective is not to treat repetition as guilt; it is to recognise that recurring allegations alter the risk picture and may require a broader investigative lens.

Learning from Disclosures

The value of a disclosure should continue after the individual case closes. Investigation findings need to translate into changed controls, clearer responsibilities, revised delegations, stronger supervision, or better training. Otherwise, the organisation has learned only who did what, not why the system allowed it. Effective remediation asks whether incentives, workload, authority, data quality, supplier arrangements or management behaviour created conditions in which the problem could occur and whether similar exposure exists elsewhere.

A useful discipline is to require every substantiated or partially substantiated case to identify root causes, affected controls, accountable owners and completion dates. Material unsubstantiated cases may deserve the same treatment where investigation reveals weaknesses despite insufficient evidence of wrongdoing. Audit and risk committees should then receive confirmation that remedial actions were implemented and, for higher-risk matters, independently tested. Closing an investigation before testing remediation can create false

assurance that the underlying risk has disappeared.

Learning should also travel horizontally. A procurement concern in one division may reveal a contract-management weakness across the group; a safety disclosure about one supplier may justify reviewing others using the same component, process, or certification. Organisations should maintain thematic action logs rather than limiting corrective action to the team named in a case. The aim is to convert local intelligence into enterprise-wide prevention before a repeated weakness produces financial, regulatory or human consequences.

Regulators similarly use disclosures beyond the immediate case. Of the 1,252 FCA whistleblowing cases closed in 2025–26, 42% led to direct action and another 53% informed wider work and harm prevention. That distinction is instructive for boards. A report need not culminate in disciplinary action or enforcement to create value; intelligence can influence supervision, training, control design, risk assessment or future testing and thereby prevent harm that would otherwise remain unseen.

A mature learning process closes the loop with the reporting population without breaching confidentiality. Employees cannot always be told detailed outcomes, but organisations can communicate anonymised themes, improvements and examples of action taken. That visibility matters because people judge reporting systems partly by observable consequences. When concerns disappear into a confidential process, and nothing seems to change, future reporters may conclude that speaking up achieves little, regardless of how professionally the original investigation was conducted.

Whistleblowing and Organisational Risk Registers

Whistleblowing themes should feed into organisational risk registers when they reveal exposure beyond a single incident. The FRC's 2024 Corporate Governance Code guidance states that risk registers can help record and monitor risks but must be reviewed and updated as circumstances change. A recurring stream of disclosures concerning fraud, safety, data, supplier integrity or management override is precisely the kind of evidence that should influence assessments of likelihood, impact, controls and risk appetite.

Public-sector practice points in the same direction. HM Treasury's Orange Book says risk management should be integral to governance, informed by timely reporting, and continually improved through learning and experience. It also expects boards to receive assessments of principal risks and control effectiveness. Speak-up intelligence should therefore be treated as one input into enterprise risk management, alongside incidents, audits, complaints, litigation, regulatory findings, operational data and external intelligence rather than as a parallel process.

Escalation should be proportionate. One allegation does not automatically justify creating a principal risk, but repeated or high-severity concerns may change the residual risk assessment or reveal that a control believed effective is failing. Boards should ask whether the risk register reflects what employees and suppliers are actually reporting. A register that remains unchanged despite repeated disclosures can become a record of management assumptions rather than a credible representation of organisational exposure.

Why Procurement Is Particularly Exposed

Procurement is particularly exposed because it sits where organisational money, individual discretion, confidential information and external commercial interests meet. Decisions about specifications, bidder access, evaluation, negotiation, variations, invoices and supplier performance can move substantial value while remaining technically complex to outsiders. UK public bodies spent an estimated £407 billion procuring goods and services in 2023–24, around one third of public-sector expenditure. Even small control failures can therefore create material aggregate consequences.

The Procurement Act 2023 reflects that exposure. For covered procurements, contracting authorities must have regard to delivering value for money, maximising public benefit, sharing information so suppliers can understand procurement policies and decisions, and acting, and

being seen to act, with integrity. Authorities must also treat suppliers equally unless different treatment is justified. These obligations make procurement integrity more than professional etiquette: it forms part of the statutory decision-making framework for public contracting.

Conflicts are another structural risk. Sections 81 to 83 of the Procurement Act require authorities to identify and keep conflicts under review, take reasonable steps to mitigate them and prepare a conflicts assessment before specified notices are published. The rules recognise personal, professional and financial interests, including potential or perceived conflicts. A whistleblower may provide information that directly affects whether an evaluation remains defensible, whether mitigation is adequate or whether a supplier must be excluded.

Competition risk adds another dimension. In 2023, the CMA fined ten construction businesses almost £60 million for colluding over demolition and asbestos-removal contracts worth approximately £150 million. Its September 2026 procurement work warns that bid-rigging can increase prices by 20% or more and may be difficult for an individual buyer to detect. Procurement professionals therefore need safe routes to report suspicious bid patterns, unusual supplier communications or pressure to ignore apparent collusion.

Private-sector procurement faces comparable vulnerabilities even where public-procurement legislation does not apply. Bribery, fraud, confidential-information leakage, kickbacks, false invoicing, supplier favouritism and undisclosed relationships can distort purchasing decisions in any organisation. The legal framework may instead involve the Bribery Act 2010, Fraud Act 2006, competition law, directors' duties, sector regulation and contractual controls. Whistleblowing is especially valuable because much procurement misconduct is designed to resemble ordinary commercial judgement until an insider explains what happened.

Commercial Pressure and Ethical Pressure

Commercial pressure becomes an ethical problem when targets allow controls to be overridden. Procurement teams routinely balance speed, continuity, savings and stakeholder expectations, but urgency can become a rationale for competition, retrospective approval, incomplete due diligence or acceptance of supplier claims that would normally be challenged. Organisations should distinguish prioritisation from pressure to bypass governance. The warning sign is not a demanding deadline; it is pressure to conceal, misstate or avoid recording the resulting decision.

Tesco's commercial-income case illustrates how performance pressure can become a governance issue. The later judicial record identified a £284 million overstatement of profit, driven by accelerated recognition of commercial income and delayed accrual of costs. Tesco Stores ultimately agreed a deferred prosecution agreement carrying a £128,992,500 financial penalty plus approximately £3 million of SFO costs. Commercial targets do not excuse weak evidence, distorted accounting judgements or reluctance to escalate uncomfortable information.

Public outsourcing provides another example. Serco Geografix entered a deferred prosecution agreement concerning electronic-monitoring contracts and paid a £19.2 million financial penalty plus approximately £3.7 million of SFO costs; Serco had previously paid £70 million in a civil settlement with the Ministry of Justice. The case involved misleading the Ministry about contract profitability. Commercial relationships become dangerous when protecting revenue or margins displaces accurate reporting and transparent dealings with the customer.

G4S Care and Justice Services later entered a separate deferred prosecution agreement over electronic-monitoring contracts, paying a £38.5 million financial penalty and roughly £5.9 million in SFO costs after a previous £121.3 million civil settlement. The SFO described fraud relating to financial reporting about profits on those contracts. The lesson is that contract management requires ethical challenge after award, not just before; misconduct can migrate from bidding into delivery and reporting.

Pressure is often transmitted down the hierarchy. A senior instruction to "get the contract

signed”, “keep the supplier on side” or “make the numbers work” may sound commercially pragmatic while creating strong incentives to suppress inconvenient evidence. Procurement leaders should explicitly protect staff who insist on approvals, challenge unexplained price movements or refuse inaccurate records. Escalation routes matter most when ordinary management channels generate the pressure that creates the ethical risk.

Targets should therefore include counterweights. Savings, speed and continuity can be measured alongside competition achieved, exceptions approved, conflicts managed, overdue actions, supplier concentration and substantiated control breaches. Executive remuneration and performance assessment should not reward outcomes achievable only by weakening governance. A successful procurement function is not one that merely spends less or buys faster; it secures defensible value while protecting the organisation from fraud, challenge, disruption and reputational damage.

Supplier Dependence

Supplier dependence can weaken challenge because the commercial consequences of confrontation appear immediate. A strategic supplier may hold specialist knowledge, proprietary technology, scarce capacity or responsibility for critical services, making replacement expensive or slow. Staff can then become reluctant to escalate poor performance, questionable charging or integrity concerns for fear of destabilising delivery. Dependency does not create wrongdoing, but it changes incentives and can make an organisation tolerate behaviour that would be challenged quickly elsewhere.

Carillion demonstrated the scale of interconnected dependency. At liquidation in January 2018, it held around 420 public-sector contracts and its supply chain was estimated to span 30,000 businesses. Parliament reported that it owed around £2 billion to suppliers, subcontractors and other short-term creditors. Standard payment terms could reach 120 days, while some suppliers faced significant discounts for quicker payment. Commercial dependence can therefore silence challenge both upstream and downstream when counterparties fear losing essential work.

Boards should respond by mapping concentration, substitutability and exit risk before concerns arise. Critical suppliers need stronger performance data, open-book rights where appropriate, contingency planning, conflict controls and escalation routes independent of relationship owners. Procurement should also monitor whether strategic status is becoming immunity from challenge. The test is simple: if the organisation would investigate identical conduct by a minor supplier but hesitates because the supplier is difficult to replace, dependency is already influencing governance.

Procurement’s Unique Visibility

Procurement professionals occupy an unusually revealing position inside organisations because they see the behaviour surrounding commercial decisions, not merely the resulting invoices or contracts. Buyers observe last-minute specification changes, pressure to include particular suppliers, unusual reluctance to compete requirements, unexplained price movements, repeated exceptions and attempts to obtain confidential information. Individually, such events may appear innocuous; together, they can provide early evidence of conflicts, collusion, fraud, bribery or management override.

That visibility continues after award. Contract managers and buyers can see repeated variations, vague consultancy charges, unusual subcontractors, unexplained commission structures, weak evidence supporting invoices and persistent requests to alter payment routes. Finance may see only an authorised transaction and legal teams only the signed contract. Procurement can often see the commercial history behind both. This makes experienced buyers an important source of intelligence about whether apparently legitimate expenditure reflects genuine value.

The Procurement Act 2023 reinforces the significance of those observations in covered public

procurement. Contracting authorities must act, and be seen to act, with integrity, treat suppliers equally unless different treatment is justified, and manage conflicts that could create unfair advantage. Suppliers may also face exclusion for improper behaviour that distorts a procurement. A buyer who notices selective information, unexplained access, or interference with evaluation may therefore be witnessing a governance issue with statutory consequences.

Visibility carries responsibility but should not turn procurement staff into investigators. Once behaviour raises reasonable suspicion, preserve records and escalate concerns through appropriate whistleblowing, legal, compliance, or fraud channels. Confronting suspected participants prematurely can alert them, compromise evidence or distort later accounts. Strong organisations therefore train buyers to recognise indicators, document facts objectively and understand where ordinary contract management ends and protected escalation or specialist investigation should begin.

Supplier Bribery

Supplier bribery can arise whenever an advantage is offered, promised, or given to improperly influence commercial judgement. Under section 1 of the Bribery Act 2010, offering, promising or giving a financial or other advantage can constitute bribery where the required connection with improper performance exists; section 2 addresses requesting, agreeing to receive or accepting such advantages. The offences can therefore capture both the person seeking influence and the recipient willing to misuse entrusted discretion.

The penalties are deliberately severe. Individuals convicted on indictment of the principal Bribery Act offences can face up to ten years' imprisonment and an unlimited fine. A relevant commercial organisation can commit the section 7 offence where an associated person bribes another intending to obtain or retain business or a business advantage for it, unless the organisation proves that adequate procedures designed to prevent bribery were in place.

Glencore Energy (UK) demonstrates the financial scale that bribery can reach. In 2022 it pleaded guilty to seven bribery counts concerning payments by agents and employees for preferential access to oil. The Serious Fraud Office recorded bribes worth more than \$25 million, and the company was ordered to pay £280 million in penalties and confiscation. The case shows bribery operating through ordinary commercial relationships, overseas markets, intermediaries and procurement-like allocation decisions.

Supplier-side bribery may be less dramatic but equally corrosive: cash, employment promises, discounted goods, home improvements, holidays, event tickets or benefits for relatives can all create improper influence. The legal question is not whether something is labelled a gift but what advantage was offered and why. Procurement controls should therefore examine context, timing, recipient influence, concealment and reciprocity rather than relying on arbitrary monetary thresholds as if they created automatic legal safety.

Public procurement adds a further consequence. Schedule 6 of the Procurement Act 2023 includes specified bribery convictions among mandatory exclusion grounds, subject to the Act's detailed rules, including relevant periods and assessment of whether circumstances are continuing or likely to recur. Bribery can therefore threaten far more than one contract: it can affect access to future public opportunities, trigger debarment scrutiny and damage the credibility on which long-term supplier relationships depend.

Bribes Disguised as Legitimate Commercial Activity

Bribes rarely arrive labelled as bribes. They can be embedded in consultancy agreements, marketing support, sponsorship, rebates, commissions, introduction fees, charitable contributions or inflated subcontract payments. The commercial description may be genuine, partly genuine or entirely fictitious. Effective control therefore asks what service was actually provided, whether pricing is proportionate, who ultimately benefited, how the intermediary was selected and whether the payment coincided with an award, approval, variation or regulatory decision.

The Sarclad deferred prosecution material illustrates the danger vividly. Of 74 contracts examined, 46 were considered suspicious and 28 implicated by specific evidence. Court material described payments called “fixed commission”, “special commission” and “additional commission” in the context of intermediary activity. The 28 implicated contracts generated £17.24 million in revenue and an estimated net profit of approximately £2.5 million. Innocent-sounding accounting labels did not remove the need to examine commercial purpose and surrounding communications.

Current Glencore proceedings provide another caution, although charges against individuals remain allegations unless proved. The Serious Fraud Office has charged former employees in connection with corrupt-payment conspiracies and alleged falsification of invoices described as service fees to a Nigerian oil consultancy. The underlying corporate case is already concluded, but the pending individual proceedings illustrate a broader control lesson: apparently routine consultancy invoices deserve scrutiny where services, counterparties, documentation or commercial rationale do not withstand examination.

Gifts and Hospitality

Gifts and hospitality are not automatically bribery. Government and prosecutorial guidance recognises that reasonable, proportionate, good-faith hospitality can be a legitimate part of business. Risk arises when an advantage is intended to induce improper performance, reward it or influence a foreign public official to obtain business or an advantage. The more lavish, concealed, poorly connected to genuine business activity, or closely timed to a decision the expenditure becomes, the more serious the concern.

Procurement requires stricter judgement because recipients can influence specifications, shortlists, evaluations, negotiations, contract extensions and performance decisions. A modest working meal after an open supplier briefing differs materially from expensive hospitality offered privately during a live competition. Value matters, but timing and influence matter just as much. Organisations should require declaration and approval rules that capture offers, not merely accepted benefits, because repeated declined invitations can themselves reveal attempts to cultivate decision-makers.

The safest control is transparency combined with proportionate restriction. Registers should record the provider, recipient, date, nature, estimated value, acceptance or refusal and relevant procurement activity. Some public-sector policies go further during tender exercises by requiring all invitations, whether accepted or declined, to be recorded and senior approval obtained before acceptance. Such controls protect employees and organisations because they create evidence that relationships were disclosed rather than concealed from scrutiny.

A policy threshold should never be mistaken for a statutory safe harbour. A £25 meal or £100 ticket does not become lawful merely because internal rules permit it, just as a higher-value event is not automatically criminal. Bribery depends on the legal elements and circumstances. Policies nevertheless help manage appearance, consistency and cumulative influence, particularly where several modest benefits from one supplier gradually create obligation, familiarity or reluctance to challenge poor performance.

Travel, Entertainment and Supplier Hospitality

Supplier-funded travel creates heightened risk because the benefit may include flights, accommodation, meals, entertainment and access unavailable through an ordinary business meeting. Legitimate expenditure can exist where travel is necessary to inspect a factory, test equipment, or understand a service, but organisations should ask who selected the itinerary, who pays, whether leisure elements are included, and whether the traveller currently influences an award, extension, dispute, or supplier-performance decision.

Ministry of Justice guidance does not prohibit bona fide hospitality or reasonable travel expenses. Its quick-start guidance expressly recognises that reasonable travel may be paid to demonstrate goods or services where proportionate to the business context. That does not

create blanket permission. Prosecutors consider factors including expenditure level, how it was provided, the recipient's influence and whether the hospitality was genuinely connected with legitimate activity or instead concealed an intention to secure improper advantage.

Timing is often decisive from a governance perspective. A supplier-funded factory visit during routine contract management may be defensible with approval and a clear business case; a luxury weekend offered days before tender evaluation is fundamentally different. Procurement policies should therefore consider procurement stage as well as monetary value. During live competition, organisations may reasonably prohibit hospitality entirely or require exceptional senior approval, removing ambiguity when impartiality must be particularly visible to competing suppliers.

Entertainment deserves similar analysis. Sporting events, concerts, hospitality boxes and destination dinners can strengthen legitimate relationships, yet they rarely provide technical information unavailable through ordinary meetings. The further an event is from a demonstrable business purpose, the harder it becomes to justify supplier funding for influential decision-makers. Repeated entertainment can also create cumulative dependence even when each occasion falls below an internal declaration threshold, making aggregate monitoring important.

International travel adds further complexity because local customs do not override UK bribery law. Facilitation payments—payments intended to induce officials to perform routine functions they are already obliged to perform—are bribes under UK guidance; the Bribery Act has no general facilitation-payment exemption. Genuine legally required administrative or official fast-track fees are different. Employees travelling for procurement or supplier management therefore need clear escalation routes when unofficial payment requests arise.

Organisations should, where practical, pay necessary travel themselves, especially for employees influencing major awards. Where supplier payment is justified, approval should precede booking and cover itinerary, class of travel, accommodation, accompanying guests, entertainment and business purpose. Records should allow later reviewers to understand why acceptance was reasonable. A defensible decision remains comfortable when disclosed to competing bidders, auditors, regulators, journalists or the organisation's own workforce.

Third-Party Intermediaries

Agents, consultants, distributors and subcontractors can extend market reach while also distancing improper payments from those benefiting commercially. Section 8 of the Bribery Act makes the Section 7 concept of an associated person functional: it covers a person performing services for or on behalf of the organisation and expressly contemplates employees, agents, and subsidiaries. Anti-bribery due diligence therefore cannot stop at payroll; commercial structures and actual service relationships matter more than labels.

Rolls-Royce provides one of the clearest UK examples of intermediary risk. Its 2017 deferred prosecution agreement addressed conduct spanning seven jurisdictions and more than two decades, with the UK resolution exceeding £497 million. The judgment recorded weaknesses in intermediary governance and noted that a 2009 compliance review found unclear accountability and inadequate enhanced due diligence in higher-risk areas. Intermediaries are not inherently improper, but unclear purpose, excessive commission and weak oversight create predictable exposure.

The most recent major example is Ultra Electronics Holdings. In May 2026, a deferred prosecution agreement required a £10 million penalty plus £4.8 million of Serious Fraud Office investigation costs after the company accepted responsibility for failing to prevent bribery connected with public-sector contracts sought through agents. The two Algerian contracts concerned were expected to generate £1.4 million profit. The resolution also requires annual compliance reports to the SFO for three years.

Whistleblowing as Anti-Bribery Intelligence

Anti-bribery controls are necessary but incomplete because bribery is deliberately concealed. Due diligence can verify corporate ownership, sanctions exposure, qualifications and public records, yet it may not reveal a private conversation, coded commission, undisclosed favour or instruction to fabricate supporting documentation. People inside procurement, sales, finance and supplier organisations may see fragments that no database contains. Whistleblowing therefore complements due diligence by capturing behavioural intelligence generated while commercial activity is actually occurring.

Glencore illustrates why human intelligence matters. Its corporate conviction concerned bribes paid through agents and employees to obtain preferential oil access, resulting in a £280 million financial penalty in the UK. Court material described cash withdrawals, intermediaries and commercial advantages spanning several jurisdictions. Sophisticated organisations can have policies, advisers, and transactional systems while misconduct remains embedded in ordinary workflows. A colleague questioning an unexplained cash request or unusual agent may therefore provide an earlier detection point.

Whistleblowing should feed anti-bribery risk assessment rather than operate separately from it. Reports concerning one agent, region, buyer, supplier or commission model should be compared with payment data, due-diligence records, hospitality registers, conflicts declarations and contract awards. Even an unsubstantiated allegation may reveal inadequate supporting records. Repeated concerns should influence risk ratings, audit sampling, intermediary reviews and decisions about whether enhanced due diligence or independent investigation is required.

The section 7 defence makes this integration particularly important. A relevant commercial organisation charged with failing to prevent bribery may defend itself by proving that adequate procedures designed to prevent bribery were in place. Ministry of Justice guidance frames prevention around proportionate procedures, top-level commitment, risk assessment, due diligence, communication and monitoring. A reporting channel that exists but is ignored, distrusted, or disconnected from remediation provides weaker evidence of an effective prevention environment.

The objective is not to turn every rumour into an accusation. Anti-bribery intelligence requires disciplined triage: preserve confidentiality, distinguish facts from suspicion, assess conflicts, secure evidence and decide whether specialist investigators or external authorities are required. Reporters should not be expected to prove the offence themselves. Their value often lies in identifying the transaction, relationship or behaviour that deserves examination before the organisation has enough evidence to determine what actually occurred.

Conflicts of Interest

A conflict of interest exists when private interests risk interfering with impartial commercial judgement. In procurement, that can involve shareholdings, outside employment, friendships, family relationships, professional connections, future employment discussions or financial interests in bidders. Conflict does not necessarily mean corruption has occurred. The governance failure arises when relevant interests are not identified, disclosed, assessed and mitigated, allowing decisions to be influenced—or reasonably perceived as influenced—by considerations unrelated to the procurement.

For covered public procurement, the Procurement Act 2023 imposes explicit duties. Contracting authorities must take all reasonable steps to identify and keep under review actual and potential conflicts, including personal, professional or financial interests that may be direct or indirect. They must mitigate conflicts and address circumstances likely to cause a reasonable person to perceive one wrongly. Conflict assessments must be prepared at prescribed stages and reviewed throughout the relevant process.

The statutory consequences can be significant. If a conflict gives a supplier an unfair advantage and that advantage cannot be avoided, or the supplier refuses necessary mitigating steps, the contracting authority must treat the supplier as excluded from that procurement.

Possible mitigation identified in government guidance includes reassigning conflicted individuals, using multiple evaluators, independent observers, management review, information equalisation and, in appropriate circumstances, cancelling and rerunning the procurement. Documentation is therefore as important as disclosure.

Whistleblowing becomes important because formal declarations depend on self-awareness and honesty. Colleagues may know that an evaluator socialises with a bidder, previously worked for the supplier, has a relative employed there or is discussing future employment, while the register remains blank. Such information should be handled carefully rather than treated as proof of misconduct. It may nevertheless justify checking declarations, restricting influence and independently reviewing affected decisions before an undisclosed interest compromises the process.

Undisclosed Supplier Relationships

Undisclosed supplier relationships can be harder to detect than gifts because the benefit may exist outside the immediate transaction. An employee might hold shares, undertake paid consultancy, have previous employment ties, expect future work or possess a family connection to a bidder. None automatically establishes wrongdoing, but each can affect—or appear to affect—objectivity. The key control is disclosing early enough for someone independent to decide whether recusal, restriction, or another mitigation is necessary.

Government conflicts guidance gives a direct example: an evaluator owning shares in a bidding supplier can create an actual conflict. In contrast, a spouse connected with a business acquiring a bidder can create a potential conflict. The guidance recommends procurement-specific declarations, checks against existing registers and public information, and confirmation from relevant teams before procurement. These controls recognise that generic annual declarations can become stale as investments, employment, family circumstances and commercial relationships change.

Future employment is especially sensitive because influence may precede any formal offer. A buyer negotiating with a strategic supplier while privately discussing a role with that organisation may face divided incentives even before remuneration begins. Organisations should therefore require declaration of active recruitment discussions where relevant to decision-making and consider cooling-off or reassignment measures. The same logic applies to consultancy work, directorships, and investments that could create personal benefit from procurement outcomes.

Historical relationships also deserve proportionate attention. Former employment with a supplier can provide valuable market knowledge and does not automatically disqualify someone from procurement activity. Risk depends on recency, seniority, continuing relationships and influence over the decision. The answer is rarely blanket exclusion; it is transparent assessment. Undisclosed history becomes more concerning where the individual shapes specifications, accesses competitor information or participates in evaluation while maintaining personal loyalties or financial connections.

Procurement technology can assist but cannot replace judgement. Conflict declarations can be linked to evaluation workflows, supplier master data and approval gates; periodic reminders can prompt updates; analytics can flag shared addresses or unusual patterns where lawful and proportionate. Yet many relevant relationships exist only in human knowledge. A colleague who raises a concern about an undeclared connection may therefore be supplying information that no automated control could reasonably discover.

When undisclosed interests are found, investigation should distinguish inadvertent omission from deliberate concealment and assess whether decisions were affected. Remediation may include recusal, rescoring, independent review, procurement cancellation, disciplinary action or external referral depending on severity. Under the Procurement Act regime, authorities must also consider whether a conflict has placed a supplier at an unfair advantage that cannot be neutralised. Protecting procurement integrity may therefore require correcting the process, not

merely updating the register.

Supplier Favouritism

Supplier favouritism can begin subtly: one bidder receives an early warning about the specification, an incumbent gets additional time, a preferred supplier receives informal coaching or evaluation weaknesses are explained away rather than scored consistently. Not every difference in treatment is unlawful; suppliers can differ in relevant respects. The governance question is whether differential treatment is objectively justified, recorded, and compatible with fair competition, rather than driven by personal preference, pressure, or undisclosed relationships.

The Procurement Act 2023 requires contracting authorities to treat suppliers the same unless differences justify different treatment, and then to take appropriate steps to ensure the difference does not create unfair advantage or disadvantage. Government training uses the example of incumbent advantage and suggests information equalisation as a possible response. Selective disclosure of commercially useful information can therefore undermine both competitive outcomes and confidence in the award's integrity.

Whistleblowing may expose favouritism before formal challenge does because insiders can see conversations and deviations that losing suppliers cannot. A buyer may notice a stakeholder rewriting requirements around one product, sharing competitor intelligence or pressing evaluators to overlook shortcomings. The appropriate response is evidence-led review: preserve communications, compare information released to bidders, test scoring consistency and examine conflicts. Preference becomes a governance failure when it displaces transparent, defensible commercial judgement.

Repeated Awards

Repeated awards to the same supplier are not inherently suspicious. Incumbents may genuinely offer better pricing, accumulated knowledge, lower transition costs, or scarce technical capability. The governance concern arises when concentration persists without convincing market evidence, competition repeatedly produces the same result despite weak performance, or exceptions steadily replace open challenge. Procurement teams should therefore analyse award patterns over time rather than judging each contract renewal, call-off or direct award entirely in isolation.

Patterns matter more when repeated awards coincide with narrow specifications, limited bidder fields, frequent withdrawals, unexplained scoring advantages, or contract extensions that avoid fresh competition. None of those indicators proves favouritism or collusion, but together they change the risk assessment. Category managers should compare award concentration against market structure, available alternatives, incumbent performance, and previous competition outcomes, and record why continued reliance remains commercially and legally defensible rather than allowing familiarity to become justification.

Public procurement data makes concentration particularly important because expenditure is substantial and repetitive. The CMA's September 2026 work on competition in public procurement emphasises that purchasing design can shape market entry, rivalry and long-term value. Repeated awards can be entirely legitimate, but authorities should consider whether procurement choices unintentionally entrench incumbents, reduce supplier diversity or make future competitions less credible, especially where switching costs and information asymmetry steadily increase with contract duration.

The correct response is challenge, not presumption. Reviewers should examine competition history, bid participation, scoring, conflicts, contract modifications, benchmarking and whether requirements have become unnecessarily supplier-specific. Where one supplier repeatedly wins, the organisation should be able to explain why using contemporaneous evidence. If employees instead observe unexplained intervention, selective treatment or resistance to testing the market, whistleblowing can provide the additional intelligence needed to distinguish

commercial success from manipulated continuity.

Declarations of Interest

Declarations of interest are essential because they force relevant people to consider personal, professional and financial relationships before influencing procurement. They are not, however, self-verifying. A blank declaration proves only that no interest was declared; it does not establish that none exists. Effective governance therefore combines declarations with reminders, procurement-specific updates, review of existing registers and proportionate verification where an individual holds significant influence over specifications, bidder access, evaluation or award decisions.

The Procurement Act 2023 reflects that wider approach. Government guidance states that contracting authorities must take all reasonable steps to identify and keep conflicts under review. Suggested measures include procurement-specific declarations, checks of pre-existing declarations and public registers, and confirmation with relevant individuals or teams. The legal duty is consequently broader than distributing a form: the authority must undertake reasonable identification activity and maintain a conflicts assessment throughout the procurement process.

Verification should remain proportionate and lawful. High-risk roles may justify checking Companies House information, published registers, prior employment disclosed through normal HR processes or known supplier relationships. At the same time, intrusive investigation without a risk basis may be inappropriate. The objective is assurance, not surveillance. Verification matters most where decision-makers can materially influence an outcome, the contract value is substantial, the market is concentrated, or allegations indicate that a declaration may be incomplete.

A declaration also requires active mitigation. If an evaluator owns shares in a bidder, disclosing the holding does not neutralise the conflict. Depending on circumstances, mitigation might involve recusal, reassignment, additional moderation, independent observation or information controls. Government guidance expressly recognises share ownership and family connections as examples requiring assessment. Governance fails when organisations treat transparency as the endpoint rather than determining whether the declared interest could still distort—or appear to distort—the decision.

Whistleblowing provides an important verification layer because colleagues may know about relationships omitted from formal records. A reporter might identify a family connection, private consultancy, future employment discussion or repeated social relationship with a supplier. Such information should trigger fair checking rather than an assumption of guilt. The value lies in testing whether the organisation's recorded conflict picture matches reality before an undisclosed interest contaminates evaluation, award or subsequent contract management.

Speaking Up About Senior Conflicts

Speaking up becomes particularly difficult when the conflicted person controls budgets, promotions, procurement strategy or access to senior leadership. Employees may reasonably fear that ordinary escalation will return the concern to the person involved. Policies should therefore provide bypass routes to an audit chair, senior independent director, designated non-executive, monitored external channel or other authority capable of acting without permission from the individual whose judgement is being questioned.

The governance problem is structural, not personal. Senior decision-makers can influence who investigates, what evidence is requested, how quickly cases move and whether findings reach the board. Even an entirely honest executive can create perceived pressure if subordinates must accuse them through a chain they control. Independent triage, protected access to records and direct reporting to non-conflicted oversight reduce the risk that organisational hierarchy determines whether a serious conflict is examined.

Where procurement is affected, delay can itself cause harm because the tender may continue,

bidders may incur cost and confidential information may circulate while the concern remains unresolved. Organisations need authority to pause relevant decisions where necessary, preserve evidence and substitute conflicted evaluators without prejudging allegations. A well-designed escalation route protects both the reporter and the accused by ensuring that seniority neither suppresses scrutiny nor converts untested suspicion into an assumed finding.

Tender Manipulation

Tender manipulation occurs when the procurement is designed or altered to steer an apparently competitive process towards a preferred outcome. Techniques can include specifications written around one product, unnecessary qualification requirements, criteria introduced to favour an incumbent, compressed timescales or procedural changes that disadvantage rivals. Legitimate technical requirements can look similar, so the critical questions are whether restrictions are objectively necessary, proportionate, disclosed and connected to the actual outcomes the organisation needs.

The Procurement Act 2023 constrains manipulation in covered procurement through rules on award criteria, assessment methodology, equal treatment and modifications. Award criteria must relate to the contract, be sufficiently clear, measurable and specific, and provide a proportionate means of assessment. Authorities must assess tenders using the published methodology and relative importance of criteria. These requirements make undocumented alterations or post-hoc preferences difficult to reconcile with a defensible competitive process.

Changes are not automatically improper. Section 31 permits modifications during a competitive procurement within defined limits, and competitive flexible procedures may allow award criteria to be refined where the tender documentation preserved that possibility. Government guidance nevertheless requires updating affected documents and giving suppliers appropriate time. Once final tendering approaches, the scope narrows substantially. Transparent change management distinguishes legitimate refinement from moving the goalposts after decision-makers have seen emerging supplier positions.

The Public Procurement Review Service's 2024–25 report shows that such concerns arise in practice. It recorded complaints about evaluation criteria, potential evaluator conflicts, incumbent bias and changes during live tender processes; where concerns were upheld, authorities were advised to improve evaluation guidance and supplier communications. The cases do not establish corruption, but they illustrate why apparently procedural complaints deserve attention: manipulation often first appears as an unexplained departure from the advertised process.

Leaking Tender Information

Leaking tender information can destroy competitive neutrality before formal evaluation begins. Budgets, competitor prices, scoring approaches, negotiation limits, clarification responses or internal views about bidder weaknesses may give one supplier an advantage unavailable to others. Some information will eventually be published or shared legitimately; the risk concerns selective or premature disclosure. Procurement teams should distinguish authorised market transparency from private intelligence that lets one participant calibrate its tender against confidential organisational knowledge.

Leaked information can be valuable even without direct payment. Knowing an undisclosed budget ceiling may allow a bidder to price just below it; receiving a competitor's figure may enable tactical undercutting; understanding evaluator concerns can allow targeted amendments. Government procurement guidance recognises pricing models, profit margins, cost build-ups and information affecting future re-bids as potentially commercially sensitive. Protection is therefore an integrity control as well as an information-governance obligation.

Competition cases demonstrate how sensitive information can facilitate wider collusion. In the household-fuels cartel case, the CMA found that competing suppliers exchanged confidential pricing and details of ongoing tenders, helping them maintain customer relationships through

market sharing and bid-rigging. One competitor supplied another with product prices before a tender, and the subsequent bid matched those figures. Information leakage can therefore harm competition even where no employee personally benefits from the disclosure.

Leaks may originate inside the buyer, within an adviser, or between competing suppliers. Investigation should therefore preserve access logs, emails, messaging records, clarification histories and document versions before confronting suspects. It should also examine whether leaked information changed bidding behaviour. A single disclosure may create an unfair advantage; repeated disclosure can support collusion or supplier favouritism. Whistleblowers often matter because they may witness conversations that technical controls record only indirectly.

For covered public procurement, improper supplier behaviour can have direct consequences. Under section 30 of the Procurement Act, a supplier that acts improperly and gains an unavoidable unfair advantage must be treated as excluded from that procurement, subject to the statutory process. Contracting authorities also have wider duties concerning equal treatment and integrity. A leak should therefore trigger consideration not only of employee conduct but also of whether the affected competition can still proceed fairly.

Prevention depends on disciplined access. Evaluation materials, budgets and competitor submissions should be available only to people who genuinely need them, with clear rules covering advisers, secondees and consultants. Bidder communications should run through controlled channels, and substantive clarifications should normally be shared consistently where relevant. Cultural controls matter equally: employees must understand that casually helping a familiar supplier can distort competition even where there is no bribe, personal gain or explicit agreement.

Manipulating Evaluation Scores

Evaluation manipulation occurs when scores are changed for reasons unrelated to the published criteria and tender evidence. Moderation legitimately allows evaluators to discuss differences and reach an agreed score, but it should not become a mechanism for reverse-engineering the desired winner. Warning signs include unexplained score movements, narrative written after the result is known, undocumented executive intervention or pressure to reinterpret evidence differently for one bidder than for another.

Under the Procurement Act 2023, the most advantageous tender must be determined by reference to the award criteria, published assessment methodology and stated relative importance of those criteria. Current guidance also requires assessment summaries to explain scores by reference to relevant information in each tender. That creates an evidential discipline: a score should be traceable to the submission and methodology rather than to preference, negotiation outside the process or retrospective attempts to justify an outcome.

Good governance preserves individual scores, moderation notes, decision histories and approved changes rather than overwriting inconvenient drafts. Independent moderation can be valuable on high-risk awards, particularly where scores shift materially, or senior stakeholders participate. Whistleblowing should remain available where evaluators believe their professional judgement has been improperly overridden. The purpose is not to prevent legitimate challenge during moderation, but to ensure every change can be explained through the agreed criteria and evidence.

Bid Rigging and Collusion

Bid rigging occurs when competitors coordinate rather than compete genuinely for work. Common forms include cover bidding, where designated losers submit deliberately unattractive tenders; bid suppression, where competitors agree not to bid; bid rotation, where winners take turns; and market allocation, where customers, territories or contract types are divided. These arrangements create the appearance of competition while removing the independent rivalry on which procurement relies to generate pressure on price, quality and

innovation.

The UK construction case the CMA concluded in 2023 provides concrete evidence. Ten suppliers of demolition and asbestos services were fined £59,334,957 after the CMA found cover bidding affecting 19 contracts worth more than £150 million. Projects included the Metropolitan Police training centre, Oxford University and Selfridges. Participating businesses agreed that some bids would be deliberately priced to lose, allowing customers to believe they had received genuine competitive alternatives.

The arrangements went further than symbolic losing bids. The CMA found that five suppliers were involved, on at least one occasion, in compensation arrangements under which designated losers would receive payments from the winner; one compensation amount exceeded £500,000. Some businesses used false invoices to conceal the payments. The conduct illustrates why procurement teams should look beyond tender documents to subsequent subcontracting, payments and relationships between supposed competitors.

The financial implications are potentially large. The CMA's September 2026 public-procurement work states that anti-competitive bid-rigging can inflate prices by 20% or more. On procurement measured in hundreds of billions of pounds, even isolated cartel activity can divert substantial public resources. Competition law therefore protects more than procedural fairness: it guards value, service quality, market entry and innovation against arrangements designed to substitute coordination for genuine rivalry.

Consequences extend beyond administrative fines. The CMA can impose penalties of up to 10% of turnover on businesses involved in cartel activity. Individuals can face criminal prosecution, up to five years' imprisonment and unlimited fines, while directors may be disqualified for up to 15 years. Under the Procurement Act 2023, cartel conduct can also support mandatory exclusion or central debarment, potentially preventing participation in covered public procurements for up to five years.

Artificial Competition

Artificial competition exists where a procurement appears to attract several independent bids, but the apparent rivalry is illusory. Suppliers may coordinate prices, submit cover bids, divide opportunities or use related entities in ways that conceal common decision-making. Common ownership alone does not automatically make separate bids unlawful; corporate groups can contain genuinely autonomous businesses. The risk arises where supposedly independent tenders are coordinated or presented in a way that misleads the buyer about competitive pressure.

Procurement teams should therefore examine economic reality rather than simply counting submissions. Three bids do not create meaningful competition if prices were coordinated, information was exchanged, or two bidders agreed that one would lose. The CMA's demolition case demonstrated precisely this deception: tenders deliberately designed to lose created an impression of genuine competition. A minimum-bid policy can even worsen risk if suppliers submit unwanted cover bids merely to remain on future tender lists.

Procurement design can also inadvertently encourage artificial competition. Closed supplier pools, repetitive tender lists and predictable award rotations may make coordination easier, especially in concentrated markets where competitors meet frequently. Authorities should vary market engagement appropriately, encourage new entry, scrutinise unexplained subcontracting between rivals and avoid practices that pressure unwilling suppliers to submit token bids. Competition should be measured by independence and contestability, not the cosmetic presence of multiple tender documents.

Connected bidders require careful, fact-specific analysis. Shared directors, addresses, ownership, or advisers may justify questions, but they do not, by themselves, establish collusion. Procurement teams should seek proportionate explanations and legal advice where necessary, preserving equal treatment and procedural fairness. Whistleblowing can be

valuable when an insider knows that separate entities share pricing decisions, exchange tender information or have agreed which entity should win, facts that corporate records alone may not reveal.

Warning Signs Procurement Teams May See First

Procurement teams may see cartel warning signs before finance, audit or senior management because they handle the bids themselves. CMA guidance identifies submissions arriving together, unusual or identical wording, identical prices, unexpectedly sparse detail, likely bidders failing to participate, the lowest bidder declining the contract and prices falling when a new entrant appears. None proves collusion, but recurring combinations deserve analysis rather than being dismissed as coincidence or ordinary market behaviour.

Other indicators arise after award. A successful bidder may subcontract substantial work to a competitor that submitted a higher tender, expected discounts may disappear simultaneously, or suppliers may rotate apparently successful territories or customers. Pricing differences may not reflect logical cost drivers such as distance or specification. Procurement professionals also sometimes hear revealing comments suggesting knowledge of competitors' bids. Those observations can be more informative when combined across several competitions and purchasing organisations.

The CMA's demolition investigation shows how apparently small anomalies can connect to serious misconduct. Evidence ultimately included emails, text messages, handwritten notes and even a notebook recording contractors alongside compensation figures. The wrongdoing affected 19 contracts worth more than £150 million over approximately five years. Detection therefore depends partly on retaining procurement records long enough to compare behaviour across time rather than treating each tender as an isolated administrative event.

Current enforcement activity reinforces the need for caution without premature conclusions. The CMA is investigating suspected bid-rigging in roofing and other construction services supplied to schools and other public and private bodies, with twelve businesses listed as under investigation in June 2026. The CMA expressly states that no one should assume competition law has been infringed. Warning signs should trigger evidence gathering, not public accusation or automatic exclusion.

Data analytics can strengthen human observation by comparing prices, timing, wording, bidder participation and award rotation across thousands of tenders. The CMA's 2026–27 plan specifically prioritises AI and data-science tools to scan public-procurement bidding data for illegal activity at scale. Local procurement teams rarely possess such a panoramic view. Their value lies in supplying contextual intelligence—commercial explanations, supplier behaviour and anomalies—that statistical detection cannot interpret reliably on its own.

The escalation protocol matters once suspicion becomes credible. Buyers should preserve bids and communications, avoid alerting suspected participants unnecessarily and seek specialist legal or competition advice. The CMA encourages reporting of suspicious cartel behaviour and offers rewards of up to £250,000 for qualifying information. Procurement professionals are not expected to establish a cartel themselves; their responsibility is to recognise unusual patterns, protect evidence and ensure information reaches people capable of assessing it properly.

Why Whistleblowing Complements Competition Controls

Competition controls increasingly use data to identify patterns humans cannot see, but analytics cannot readily explain motive, private conversations or concealed relationships. A pricing algorithm may flag suspicious similarity; a whistleblower may know that competitors met beforehand, exchanged spreadsheets or agreed who should win. These sources of intelligence are complementary. Data provides scale and consistency, while human reporting supplies context that can transform an anomaly from a statistical curiosity into an investigable hypothesis.

The CMA explicitly recognises the importance of human intelligence by offering rewards of up to £250,000 for useful cartel information. Its guidance explains that cartels are secret and difficult to detect and prove. At the same time, the authority is expanding AI-enabled bid-rigging detection across public procurement. Together, they capture two different evidential strengths: technology can identify unusual patterns across markets, while insiders can reveal the communications and agreements that produced them.

Organisations should therefore connect whistleblowing, procurement analytics, fraud controls and competition-law escalation rather than operating them as separate systems. A suspicious bid pattern may justify checking disclosures; a whistleblowing report may justify retrospective data analysis across tenders. Neither source should be treated as proof on its own. The strongest control environment combines detection with protected human challenge, ensuring that concealed coordination has fewer places to hide and that legitimate supplier behaviour is not mischaracterised without evidence.

Invoice Fraud

Invoice fraud ranges from deliberately false bills to inflated quantities, altered prices and duplicate claims for the same supply. The Fraud Act 2006 may apply where a person dishonestly makes a false representation intending to make a gain or cause loss. Procurement and accounts-payable controls should therefore establish not merely that an invoice looks plausible, but that the supplier, purchase, price, delivery and authorisation each correspond to genuine underlying activity.

The scale of the surrounding fraud threat is considerable. The Government's 2026 Fraud Strategy estimates the economic and social cost of fraud affecting individuals and businesses in England and Wales at at least £14.4 billion in 2023–24, including £5.2 billion affecting businesses. Procurement fraud represents only part of that total, but invoicing systems are attractive because legitimate organisations already process large volumes of routine, time-sensitive payments.

Duplicate payments illustrate how error and fraud can exploit the same weakness. The National Fraud Initiative reported £11 million of outcomes from trade-creditor and procurement matching in 2022–24. Luton Borough Council identified a duplicate payment of £34,000 involving similarly named creditors and recovered the money after threatening legal action. Duplicate-detection controls therefore protect against deliberate abuse while also identifying process failures that can generate substantial accidental loss.

Technology helps, but simple matching rules are imperfect. Northern Ireland's 2022–24 National Fraud Initiative identified 28 duplicate payments and recovered £90,475; one £6,456.26 duplication escaped internal detection because the invoice was keyed once in uppercase and once in lowercase, while another £23,167 duplicate involved an altered reference digit. Effective analytics should therefore use supplier, amount, date, bank-account and purchase-order patterns rather than relying solely on exact invoice-number matching.

Phantom Services

Phantom-service fraud occurs when an organisation pays for work that was never performed, was materially less extensive than claimed or cannot be evidenced at all. It thrives where invoice approval is treated as an administrative step rather than confirmation of delivery. Three-way matching between purchase order, receipt and invoice can reduce exposure, but service contracts need equally strong evidence: timesheets, outputs, site records, milestones, performance data and accountable confirmation that work occurred.

The legal distinction between weak evidence and fraud matters. Poor record-keeping does not prove dishonesty, whereas knowingly invoicing for services never delivered may support a fraud allegation under the Fraud Act 2006. An employee who dishonestly approves fictitious work while expected to safeguard the organisation's financial interests may also engage in fraud by abuse of position. Investigations should therefore establish who represented what,

what was actually supplied and what each participant knew.

Dorset Council's 2025 health-and-safety compliance investigation provides a recent governance example. Its published findings identified inflated costs, duplicate invoices and unverified services, including charges of £300 for services said to be worth only £20 and work undertaken at non-council sites without justification. The findings also described inadequate verification of goods and services. Even when an irregularity is not criminal fraud, weak evidence creates the environment in which phantom work can survive.

Mid Essex Hospital Services NHS Trust provides a particularly direct phantom-services case. Its former Head of Unified Communications, Barry Stannard, submitted invoices through two companies he controlled. However, the NHS Counter Fraud Authority found that those companies never supplied any of the products or services invoiced. The total fraud against the NHS and HMRC reached £806,229.80, and Stannard was sentenced to five years and four months' imprisonment.

Whistleblowing can detect what document matching cannot. A colleague may know that engineers never attended, consultancy meetings never occurred or reported maintenance could not have been completed. Compare those observations with access records, delivery evidence, diaries, system logs, and customer outcomes. Organisations should also analyse repeated round-sum invoices, vague descriptions and services approved by the same individual who commissioned them, particularly where physical or measurable evidence of performance is unexpectedly absent.

Purchase Order Manipulation

Purchase orders are preventive controls because they require expenditure to be authorised before commitment, define what is being bought and create a reference against which invoices can be matched. Manipulation occurs when users invent order numbers, alter quantities after approval, attach unrelated invoices or exploit emergency routes to make unauthorised spending appear legitimate. The control is weakened further where the same person can create suppliers, raise orders, confirm receipt and approve payment.

HMRC's electronic-invoicing guidance illustrates the principle of segregation. It identifies procedural controls such as requiring a purchase order before receiving an invoice and authorisation controls that prevent a user who maintains supplier master data from entering invoices for that supplier. These are not universal statutory prescriptions for every organisation, but they demonstrate a basic control architecture: no individual should be able to create both the commercial authority and the accounting evidence needed to release money.

Herefordshire Council's current counter-fraud guidance lists false purchase orders and contract variation orders among examples of procurement and contract fraud. That classification is useful because purchase-order abuse can be either an attempt to regularise genuine but unauthorised expenditure or part of a deliberate scheme involving fictitious suppliers, false invoices or diversion of funds. Investigators should therefore examine intent, supporting evidence and system history rather than assuming every irregular order is merely poor administration.

Splitting Expenditure

Splitting expenditure means dividing what is substantively one requirement into smaller purchases so each falls below a competition, approval, or reporting threshold. Legitimate phased requirements and genuinely separate contracts are not automatically problematic. The concern arises when subdivision is designed to avoid governance that would have applied to the combined need. Repeated low-value orders to one supplier, particularly over short periods, should therefore be analysed collectively rather than approved transaction by transaction.

For contracting authorities, the Procurement Act 2023 directly addresses deliberate threshold avoidance. Section 4 requires estimated contract values to follow statutory valuation rules and

states that authorities must not manipulate estimated value to exclude a contract from the Act's requirements. Official learning materials likewise tell authorities to confirm total estimated value while ensuring contracts are not artificially subdivided. Splitting is therefore not simply an internal-policy issue where statutory coverage would otherwise apply.

Internal delegation thresholds create a separate risk in public and private organisations. Ten purchases of £9,500 may each appear compliant with a £10,000 approval limit while representing a £95,000 commitment that senior management never reviewed. Analytics should identify cumulative spend by supplier, category, requester and period, including purchase cards and non-order invoices. Whistleblowers can add context by explaining whether apparently separate purchases were planned together or deliberately sequenced to remain below controls.

The NHS case identified through National Fraud Initiative matching demonstrates how threshold knowledge can be exploited. An IT manager at an Essex hospital trust generated fraudulent invoices through two undeclared companies, keeping each below his £7,500 authorisation limit, and obtained £674,000. He added £132,000 of VAT to make invoices appear plausible and was sentenced to five years and four months' imprisonment. Repeated sub-threshold activity can therefore be a behavioural signature.

Retrospective Purchase Orders

A retrospective purchase order is raised after goods or services have already been ordered or delivered. It can be legitimate where an authorised emergency required immediate action, but routine retrospective ordering removes the purchase order's preventive purpose. Approval becomes confirmation of a fait accompli rather than a decision about whether expenditure should occur. Repeated use can conceal unauthorised commitments, supplier favouritism, contract leakage, deliberately avoided competition or invoices created without valid prior authority.

The Home Office illustrates the opposite control model through its published "no purchase order, no payment" approach. Suppliers are instructed to accept requests only when supported by a valid purchase order, and to reject invoices without the required number. Such policies are not universal legal requirements, but they create a clean sequence: approval first, commitment second, delivery third and payment last. Retrospective ordering reverses that sequence and transfers leverage from purchaser to supplier.

Retrospective orders also weaken financial forecasting because liabilities exist before systems record them. Budget holders may believe funds remain available while employees have already committed expenditure elsewhere. At year-end, the problem can become particularly acute as organisations discover unrecorded liabilities or rush to regularise commitments. Strong management information should therefore distinguish genuinely pre-authorised orders from purchase orders created after invoice receipt, allowing boards and audit committees to see the scale of exceptions.

Fraud risk increases when retrospective ordering becomes culturally normal. A dishonest employee can purchase from a connected supplier, arrange delivery and then pressure approvers to regularise the transaction because cancelling it would be inconvenient. Even without fraud, the same behaviour undermines segregation of duties and competitive challenge. Approval data should therefore record original commitment dates, requisition dates, purchase-order creation and invoice dates, enabling analytics to identify systematic backdating or persistent late ordering.

Dorset Council's 2025 investigation demonstrates how apparently administrative weaknesses can accumulate into governance failure. Its findings described direct awards without recorded due diligence, subcontracting approved outside formal procurement processes, missing decision records, work-order increases used to avoid appropriate oversight and payments authorised inconsistently with delegated authority. The significance lies in combination: procurement exceptions, weak documentation and payment-control failures can reinforce one

another, making improper expenditure progressively harder to challenge once commitments have already been made.

Whistleblowers are valuable where system data shows only that an order was late, not why. Staff may know that a supplier began work before approval, that management instructed buyers to “sort the paperwork later”, or that supposed urgency was manufactured to avoid competition. Reporting routes should therefore allow concerns about repeated retrospective procurement to reach finance, procurement, internal audit, or counter-fraud teams without requiring employees to accuse colleagues of criminal conduct first.

Supplier Bank-Account Changes

Supplier bank-account changes are a critical payment-fraud control because criminals can leave every other element of a genuine invoice untouched while redirecting the money. UK Finance defines invoice-and-mandate scams as cases where a victim intends to pay a legitimate payee but is persuaded to send funds to an account controlled by criminals. In 2025, these scams caused £41.3 million in losses across personal and non-personal accounts, despite a 4% annual reduction.

Verification should therefore occur outside the change request itself. Government fraud guidance advises organisations to confirm new bank details directly with the supplier using contact information that has been reliably used previously, not telephone numbers or email details supplied in the message requesting the alteration. Dual authorisation, callback records, cooling-off periods for high-value changes and alerts to existing supplier contacts can add further protection against compromised email accounts and impersonation.

Whistleblowing remains relevant because insiders may notice unusual urgency, repeated account changes, bypassed callbacks or requests to ignore verification procedures. The strongest control separates supplier master-data amendments from payment approval and retains an audit trail of who requested, checked, and authorised each change. Where a payment has already been misdirected, immediate contact with the organisation’s bank and fraud-reporting channels can be crucial because recovery prospects generally deteriorate as stolen funds are moved onward.

Fraudulent Supplier Creation

Fraudulent supplier creation occurs when fictitious or misrepresented entities are added to payment systems so that false invoices can be processed through apparently normal workflows. The danger increases where supplier setup relies on documents supplied by the requester without independent validation. Basic checks should establish legal identity, address, tax information where relevant, bank-account ownership, business purpose and the internal sponsor. At the same time, segregation prevents the person requesting creation from unilaterally approving subsequent payments.

Mid Essex Hospital Services NHS Trust provides a named example of fraudulent supplier use. Barry Stannard, its Head of Unified Communications, controlled two companies that invoiced the trust although no products or services were ever supplied. The NHS Counter Fraud Authority recorded a total fraud of £806,229.80, including more than £132,000 of improperly charged VAT. Data matching between payroll, accounts payable and Companies House exposed the undeclared supplier connections.

The control response should be structural, not cosmetic. Supplier creation should require independent validation of identity, bank details and business need, with segregation between onboarding, purchase approval and payment. HMRC’s electronic-invoicing guidance similarly gives an example of an authorisation control preventing a user who maintains supplier master data from entering invoices for that supplier. Stopping only the final payment leaves the underlying route available for another fraudulent attempt.

Modern supplier onboarding can use Companies House records, sanctions screening, tax checks, banking verification and beneficial-ownership information, but automation should not

be mistaken for proof. Genuine companies can be hijacked, shell entities can be lawfully incorporated and apparently correct documents can be fabricated. The central question remains whether the proposed supplier has a legitimate commercial relationship with the organisation and whether its ownership, account details, and capabilities align with the proposed transaction.

Whistleblowers may identify inconsistencies before automated controls do: a supplier nobody recognises, invoices for unfamiliar services, a residential address linked to an employee or repeated payments to an entity with no visible operational presence. Such reports should trigger controlled review of master data, purchase history, bank information and connected persons. Where suspicion concerns internal involvement, access logs are especially important because they can show who created, amended, approved or repeatedly interacted with the supplier record.

Employee-Controlled Suppliers

Employee-controlled suppliers create a direct conflict between purchasing authority and personal financial interest. The connection may involve formal directorship, beneficial ownership, a spouse or relative, or effective control exercised through another person. Such relationships are not always prohibited, but undisclosed participation in supplier selection, ordering, receipt or payment can make impartiality impossible to demonstrate. Controls should therefore link declarations of interest with supplier-master data and Companies House information where proportionate.

The National Fraud Initiative provides a stark NHS example. Payroll-to-Companies House matching identified an Essex hospital-trust IT manager as the sole director of two undeclared companies. Investigators found he had used fictitious employees to send fraudulent invoices, all below his £7,500 authorisation limit, obtaining £674,000 from the trust and adding £132,000 of VAT. He was dismissed, prosecuted and sentenced to five years and four months' imprisonment. Data matching exposed what declarations had not.

A Northern Ireland Audit Office procurement-fraud guide records another connected-supplier case in local government. A housing employee colluded with her husband's cleaning business, helping inflate charges and directing work towards it. A supplier initially added for a £900 one-off job received £126,000 over a year, despite procurement rules requiring expenditure above £10,000 to be tendered and contracted. Spend analysis exposed both the undeclared relationship and the absence of competition.

Verification need not assume wrongdoing whenever an employee shares a surname or address with a supplier. Matching produces leads, not verdicts, and false positives require careful review. The objective is to detect relationships early enough for disclosure, recusal and independent approval. Where an employee concealed ownership and influenced purchases or payments, investigators should preserve corporate records, system histories, bank information and communications because the conflict may extend beyond procurement policy into fraud.

Tender Confidentiality

Tender confidentiality protects the integrity of competition and suppliers' legitimate commercial interests. Bid documents can contain pricing models, technical methods, intellectual property, staffing structures and strategic assumptions that competitors could exploit. Access should therefore be controlled before, during and after evaluation. The principle is not secrecy for its own sake: procurement must also deliver appropriate transparency, especially in the public sector. Confidentiality and transparency require disciplined classification rather than blanket treatment.

For covered public procurement, section 12 of the Procurement Act 2023 requires authorities to consider sharing information so suppliers can understand procurement policies and decisions while also acting, and being seen to act, with integrity. Equal treatment is required

unless relevant differences justify otherwise. Selectively revealing one bidder's tender to another would therefore raise concerns beyond confidentiality because unequal informational advantage can compromise the legitimacy of the competitive process itself.

Section 94 provides a specific public-procurement safeguard. Authorities may withhold information they would otherwise have to publish or disclose where it is sensitive commercial information and an overriding public interest favours withholding it. The statutory definition covers trade secrets and information whose disclosure would likely prejudice commercial interests. This does not permit automatic secrecy: authorities must assess the information and applicable public interest rather than accept a supplier's confidentiality label.

Freedom of information creates a parallel discipline for public authorities. The Information Commissioner recognises that tender submissions, contracts and procurement plans may contain commercially sensitive information, but section 43 of the Freedom of Information Act 2000 requires the relevant exemption tests to be satisfied. A contractual confidentiality clause does not automatically prevent disclosure. Public bodies therefore need procurement records that can separate genuinely sensitive content from information that should properly be transparent.

Private organisations also have reason to protect bids carefully. The Trade Secrets (Enforcement, etc.) Regulations 2018 define a trade secret as secret information with commercial value because of its secrecy and that it has been subject to reasonable protective steps. Tender material will not automatically meet that definition, but unique pricing structures, methodologies or technical solutions may. Access controls, confidentiality terms and secure procurement platforms can therefore support both commercial trust and legal protection.

Whistleblowing becomes relevant where employees see bid documents forwarded informally, competitor prices discussed with preferred suppliers or evaluation material accessed without business need. System permissions and audit logs can show who opened documents, but they rarely explain why information was shared or what was said afterwards. Protected human reporting fills that gap. Investigators should preserve access histories, emails, messaging records and document versions while avoiding unnecessary circulation of the sensitive information under investigation.

Information Leaks

Information leaks can be deliberate, careless or simply the product of weak information discipline. Procurement teams hold budgets, pricing, technical proposals, evaluation records, negotiation positions and supplier strategies whose premature disclosure can alter competitive behaviour. A confidential document forwarded to a personal account, an evaluator discussing bids informally or a presentation left accessible on a shared drive may create commercial advantage even where nobody intended corruption or personal gain.

The legal and governance consequences depend on what was disclosed and why. For covered public procurement, the Procurement Act 2023 balances transparency with protection for sensitive commercial information, including trade secrets and information whose disclosure would likely prejudice commercial interests. Private organisations may also owe contractual, confidentiality, data-protection or trade-secret obligations. The important control question is therefore not whether information was marked confidential, but whether disclosure was authorised, necessary and appropriately controlled.

Carelessness deserves attention because repeated low-level leakage can normalise behaviour that deliberate actors later exploit. Sending tender documents to broad distribution lists, discussing supplier pricing in open offices or retaining access after leaving an evaluation team all increase exposure. Organisations should classify sensitive material, restrict access by role and review permissions throughout the procurement lifecycle. Whistleblowing becomes important when employees see established controls ignored repeatedly or information deliberately channelled towards preferred external parties.

Investigation should distinguish mistake from misconduct without understating either. Relevant evidence may include emails, download histories, collaboration-platform logs, document versions, printing records and witness accounts. Investigators should establish what information left the controlled environment, who received it, whether bidding or negotiation behaviour changed and whether similar incidents occurred previously. An apparently minor disclosure can matter disproportionately if it gives one supplier information unavailable to competitors at a commercially decisive moment.

Using Insider Information to Advantage a Supplier

Insider information can distort competition without resembling conventional bribery. Telling a supplier the buyer's undisclosed budget, a competitor's likely price, an evaluator's concerns or the weighting being considered for revised criteria can allow that supplier to reshape its offer around knowledge others do not possess. The disclosure may take seconds and involve no payment, yet it can change who wins a contract worth millions of pounds and undermine the credibility of the entire competition.

The distortion is particularly serious where information reveals the organisation's negotiating boundary. A bidder told that £4.8 million is acceptable when the published requirement disclosed no budget may have little incentive to offer £4.2 million. A supplier privately advised that its quality response is weak can repair shortcomings that competitors must identify themselves. Competition depends on bidders responding independently to common information; selective intelligence replaces market rivalry with privileged access.

For covered public procurement, contracting authorities must treat suppliers the same unless differences justify different treatment and steps prevent unfair advantage. They must also have regard to acting, and being seen to act, with integrity. Those principles make informal assistance potentially significant. Where one supplier receives material information unavailable to others, the authority should consider whether equalisation, mitigation, exclusion or restarting the affected stage is required rather than simply asking the recipient to ignore it.

Competition law can also become relevant where commercially sensitive information moves between competitors. The CMA's household-fuels cartel case found exchanges of confidential pricing and tender information that supported market sharing and bid-rigging. One competitor supplied another with product prices before a tender, and the subsequent competing bid reflected those figures. The example demonstrates how information exchange can provide the mechanism through which apparently separate suppliers cease competing independently.

Whistleblowers can expose the human context behind ambiguous data. System records may show that an employee opened a tender file, but only a colleague may know that the contents were later discussed with a supplier during a private meeting. Reports should therefore be assessed alongside access logs, communications and subsequent bid behaviour. The objective is to establish whether legitimate access became improper use, not to infer wrongdoing merely because an authorised user viewed sensitive material.

Data Access and Audit Trails

Audit trails transform suspicion into testable evidence. Procurement and enterprise systems can record who viewed, created, downloaded, amended or approved information, when activity occurred and sometimes from which device or location. Those records help investigators distinguish authorised work from unexplained access and reconstruct events after an allegation. They are especially useful where several employees legitimately possess system permissions, because access rights alone do not establish whether a particular action served a genuine business purpose.

Logs must themselves be governed properly. Retention periods should reflect operational, legal, investigative and security needs; privileged access should be restricted; and administrators should not be able to erase evidence casually. Reviews can focus on unusual downloads, access outside working patterns, repeated viewing of competitors' submissions or

activity shortly before suspicious supplier communications. Automated alerts can strengthen controls, but high-risk flags still require contextual assessment before conclusions are drawn.

Human intelligence remains necessary because digital evidence rarely captures motive. A download could support legitimate evaluation, while a screen photograph might leave no corresponding file transfer. Conversely, an allegation may be disproved by logs showing that the accused employee never accessed the relevant information. Combining whistleblowing with system evidence therefore protects both the organisation and individuals: credible concerns can be investigated rigorously while speculation is tested against objective records rather than repeated as fact.

Beyond the Immediate Supplier

Tier One visibility is rarely sufficient where labour, raw materials, components or environmental impacts sit deeper within the supply chain. A direct supplier may have strong policies and modern offices while relying on subcontractors, labour brokers or manufacturers operating under very different conditions. UK government modern-slavery guidance explicitly recognises that risks can exist further down supply chains where visibility and regulation are weaker and, depending on risk, mapping may need to extend to source.

The commercial structure can obscure accountability. A facilities contractor may subcontract cleaning through a labour provider using another recruitment intermediary. An electronics distributor may buy finished assemblies containing minerals, batteries or components sourced through several countries and businesses. Each additional tier separates the buyer from workers and production conditions. Assurance based solely on the Tier One supplier can therefore confirm the quality of relationship management without establishing what is happening where risk actually arises.

PPN 009 requires in-scope central government bodies to identify and manage modern-slavery risks in supply chains and recommends proportionate mapping where risk warrants it. The guidance suggests beginning with Tier One and moving beyond it where the direct supplier cannot provide sufficient assurance, extending to source where sector, country or commodity risk justifies it. Private-sector buyers carry no equivalent statutory duty, but the same risk-based mapping principle remains sound commercial due diligence regardless of sector.

Whistleblowing extends that visibility because disclosures can originate below the contractual interface. Subcontractor employees, agency workers, logistics staff or supplier managers may identify conditions that never appear in Tier One reports. Organisations should therefore consider whether reporting channels are accessible beyond their own employees and whether contract clauses require suppliers to permit escalation. A supply chain cannot be considered transparent merely because the buyer knows the name of the business issuing its invoice.

Modern Slavery and Labour Exploitation

That deeper visibility matters most for labour, where modern slavery is a current UK risk, not a problem confined overseas. In 2025, 23,411 potential victims were referred into the National Referral Mechanism, 22% more than in 2024. Seventy per cent were adults at referral and 30% children. UK nationals were the largest nationality group, accounting for 5,110 referrals, demonstrating that exploitation can be domestic as well as imported through supply chains.

Labour exploitation is especially relevant to procurement because commercial pressure can transmit harmful incentives down the chain. Government guidance warns buyers to consider short lead times, late payments, demands for flexibility and downward cost pressure because suppliers may recover commercial concessions through labour practices. Extremely low labour prices deserve scrutiny where statutory wages, tax, accommodation, transport and supervisory costs make lawful delivery economically implausible. Cheap supply can sometimes reflect efficiency; it can also conceal exploitation.

The 2025 Duty to Notify data reinforces the labour dimension. The Home Office received 7,130 reports concerning adult potential victims who did not consent to enter the National Referral

Mechanism. Labour exploitation was the most common exploitation type, appearing in 3,216 reports, or 45%. These statistics concern potential victims rather than proven offences, but they illustrate the scale reaching public authorities and why organisations should not equate absent supplier disclosure with absent risk.

Section 54 of the Modern Slavery Act 2015 requires qualifying commercial organisations supplying goods or services, carrying on business in the UK and having turnover of at least £36 million to publish a slavery and human-trafficking statement. The obligation promotes transparency but does not itself prove effective due diligence. A polished statement can describe policies while exploitation remains hidden several tiers below, making worker intelligence, purchasing practice and remediation capability more important than publication alone.

Worker voice is therefore a critical complement to audits. Updated Home Office guidance states that audits should not be relied upon alone and should be supplemented by worker-centred practices, worker associations and representatives, including trade unions. Workers may know who retained passports, imposed illegal deductions, threatened dismissal or demanded excessive hours. An auditor visiting for one day may see tidy records; employees experience the employment relationship continuously and can identify discrepancies between paperwork and reality.

The governance response should prioritise protection and remediation as well as evidence preservation. Abrupt termination may remove a supplier from the buyer's risk register while leaving vulnerable workers unemployed, indebted or exposed to retaliation. Government procurement guidance includes remedial action planning because buyers should consider how to correct exploitation safely. Whistleblowing intelligence is most valuable when it leads not merely to contractual distancing, but to action that addresses the conditions allowing exploitation to continue.

Human-Rights Abuses Below Tier One

The same dynamic that hides slavery can hide wider abuse: human-rights risk often intensifies below Tier One because commercial visibility decreases while labour-intensive activity increases. Subcontractors may operate in jurisdictions with weaker enforcement, use temporary labour or outsource again to smaller workshops, farms, mines or recruitment agents. Government guidance recommends systematic, progressive supply-chain mapping rather than assuming contractual assurances at the first tier accurately describe every underlying workplace.

The risk is not limited to modern slavery. Excessive hours, withheld wages, discrimination, unsafe accommodation, restrictions on association and abusive supervision can occur without satisfying the legal definition of forced labour. Procurement due diligence should therefore consider wider labour standards and grievance information alongside formal modern-slavery indicators. A supplier may truthfully report no identified slavery cases while still operating a subcontracting model that creates vulnerability, weakens worker bargaining power and discourages reporting.

Whistleblowing can reconnect buyers with those hidden layers. A worker several tiers removed may know that production was moved to an unauthorised site, wages are being withheld or passports have been confiscated. Contractual reporting routes rarely reach that person automatically. Effective programmes use multilingual channels, worker interviews, trusted civil-society partners and escalation mechanisms that do not depend solely on line management. Visibility improves when organisations ask workers directly rather than relying exclusively on supplier-generated assurance.

Recruitment Fees and Debt Bondage

That hidden abuse often begins with recruitment, before a worker even reaches the workplace. UK government guidance warns that workers may be charged fees by labour brokers, take on

debt to secure employment or surrender identity documents during recruitment. Multiple intermediaries can each charge a fee, leaving migrants owing substantial sums before earning wages. Debt then changes the worker's freedom to leave poor conditions because repaying the loan may threaten family property or safety.

The GLAA identifies debt bondage, withheld earnings, retained identity documents and debts for transport or accommodation among indicators of trafficking and forced labour. These signs may remain invisible in payroll data because the debt can exist in the worker's country of origin or be collected informally. A payslip showing lawful gross pay therefore does not establish that the employee retained genuine control of their earnings or entered the employment relationship freely.

Government procurement guidance recommends asking workers directly whether recruitment fees were paid, prohibiting labour providers from charging such fees, checking migrant workers have not had identity documents retained and providing confidential processes through which fee payments can be reported and remediated. These controls recognise an important limitation of supplier questionnaires: a labour provider engaged in abusive recruitment is unlikely to describe that abuse accurately merely because a buyer asks it to complete a compliance form.

Price analysis can also expose risk. The GLAA publishes indicative minimum labour-provider charge rates reflecting statutory employment costs and basic overheads, excluding profit. It warns that businesses supplying labour below plausible minimum rates may be cutting corners at workers' expense or evading tax. Procurement teams should therefore challenge bids whose economics appear inconsistent with lawful employment, particularly where labour represents most of the contract cost and unexplained savings are substantial.

Whistleblowers can reveal the financial arrangements behind superficially compliant employment. Workers may explain that wages are diverted to recruiters, deposits are demanded, passports are withheld or repayment obligations continue for months. Reports should be handled sensitively because immediate confrontation with the labour provider can expose workers to retaliation. Remediation may require specialist modern-slavery advice, repayment of recruitment fees, protection from dismissal and engagement with competent authorities rather than ordinary supplier-performance procedures.

Child Labour and Forced Labour

Debt bondage often shades into the most severe categories of exploitation: child labour and forced labour remain major global supply-chain risks. International Labour Organization data records 160 million children in child labour in the 2020 global estimate and 27.6 million people in forced labour in 2021. Those figures do not imply every international supply chain is affected, but they explain why buyers cannot treat legal prohibitions in supplier codes as sufficient evidence of compliance.

The UK picture also requires nuance. Of 23,411 people referred to the National Referral Mechanism in 2025, 7,028 were children at the point of referral. Referral indicates potential victimhood rather than a final finding, and exploitation types vary, but the figure demonstrates that children remain materially represented in the UK safeguarding system. Procurement professionals should recognise that exploitation can arise through domestic subcontracting and services as well as imported goods and overseas manufacturing.

Direct worker voice matters because documentary assurance can be staged. Age records may be falsified, employees coached before an audit or forced workers kept away from visitors. Interviews conducted safely, in workers' own languages and without supervisors present can reveal recruitment routes, working hours, restrictions on movement and threats that personnel files omit. Home Office guidance specifically recommends engaging vulnerable workers and cautions against relying on audits alone as the source of modern-slavery intelligence.

The response to credible evidence must protect victims rather than simply protect the buyer's

reputation. Immediate supplier termination can sometimes worsen harm by removing wages, accommodation or access to remediation. Risk-based plans should consider safeguarding, repayment, lawful employment, responsible disengagement and referral to appropriate authorities. Whistleblowers should not be expected to investigate trafficking themselves; their role is to identify concerns so trained organisations can establish facts and protect affected people.

Migrant Workers and Vulnerability

The same dependency recurs, in sharper form, among migrant workers, whose employment, accommodation, immigration status, transport and language may become concentrated in the hands of one employer or intermediary. Dependence increases when changing jobs risks losing accommodation or lawful status, or when workers do not understand UK employment rights. This does not make migrant employment exploitative, but it can widen the power imbalance that allows underpayment, coercion or unsafe conditions to persist without complaint.

The GLAA's exploitation indicators include workers lacking possession of passports, having movements controlled, living in accommodation chosen by others, receiving little or no pay, lacking access to earnings or believing themselves bonded by debt. No single indicator proves modern slavery, and the GLAA stresses that circumstances must be considered individually. Procurement teams should therefore avoid crude profiling while remaining alert to combinations of dependency that may warrant specialist assessment.

Language can determine whether a speak-up channel exists in practice. A hotline advertised only in English is of limited value to workers who cannot understand the instructions, while written procedures may exclude those with low literacy. Organisations buying labour-intensive services should consider multilingual reporting, interpretation, visual guidance and trusted intermediaries. Confidentiality should be explained because workers unfamiliar with UK systems may assume any complaint will automatically be disclosed to their supervisor, recruiter or immigration authorities.

Immigration status can intensify fear, even when workers have lawful rights. Unscrupulous employers may threaten dismissal, deportation or reporting to authorities, regardless of whether such threats accurately reflect the law. Workers whose visa or recruitment arrangements are closely tied to employment may have little practical freedom to challenge conditions. Independent reporting routes are therefore especially important where the employer, sponsor, accommodation provider and transport organiser are effectively the same commercial network.

UK public procurement guidance specifically recommends checking with migrant workers on arrival that recruitment fees have not been charged and identity documents have not been retained. This is significant because supplier management normally focuses on organisational representatives rather than individual workers. Asking the workforce directly changes the evidence base. It also helps identify exploitation before it becomes visible through absenteeism, accidents, regulatory intervention or criminal investigation.

Whistleblowing systems should not require workers to understand legal terminology. A report that "my passport is held", "I owe the recruiter money" or "I cannot leave this accommodation" may be more useful than an allegation labelled modern slavery. Triage teams should recognise these indicators, protect the reporter and seek specialist advice. The burden of legal classification belongs with trained investigators and authorities, not with vulnerable workers attempting to describe what is happening to them.

Health-and-Safety Failures

Labour exploitation is not the only hazard workers are best placed to see: unsafe practices can persist when employees believe production, deadlines or cost targets matter more than reporting hazards. Workers may see guards removed from machinery, maintenance deferred,

near misses concealed or subcontractors instructed to continue despite unsafe conditions. In Great Britain, 126 workers were killed in work-related accidents during 2025–26, including 25 in construction, 22 in agriculture and 18 in manufacturing.

The wider burden extends far beyond fatalities. HSE reports 1.9 million working people suffering work-related illness in 2024–25, 680,000 sustaining workplace injuries according to the Labour Force Survey and 40.1 million working days lost through work-related illness and injury. The estimated economic cost of injuries and ill health from current working conditions reached £22.9 billion in 2023–24. Suppressing safety information can therefore carry substantial human and financial consequences.

Whistleblowing is particularly valuable where formal safety metrics are distorted. A site can report improving incident rates because employees have been discouraged from recording near misses, injuries are reclassified, or subcontractor incidents remain outside internal dashboards. Boards should compare speak-up reports with RIDDOR data, absence, insurance claims, maintenance records and contractor information. A falling reported accident rate deserves celebration only when there is evidence that reporting confidence and hazard visibility have not fallen with it.

Product Safety and Quality Manipulation

The same gap between paperwork and reality that hides safety incidents also disguises unsafe products: failures can begin long before a regulator or purchaser sees the finished item. Employees may witness substituted materials, omitted inspections, altered settings or quality records completed without testing. Assurance systems commonly rely on documentation generated by the manufacturer itself, so when records are manipulated, purchasing checks can confirm compliance while the physical product no longer matches the evidence.

The Office for Product Safety and Standards received 2,396 Product Safety Database notifications during 2025–26 covering 3,368 notified products. Of the notifications, 563 were recorded as presenting a serious risk and 259 as high risk. Among 3,368 products notified, 2,072 had at least one corrective action recorded, including 479 recall actions from end users. The figures are notifications, not an estimate of all unsafe products, but they illustrate regulatory activity.

Grenfell provides the gravest UK illustration of product-assurance failure. The Phase 2 Inquiry reported systematic dishonesty by manufacturers involving deliberate manipulation of testing processes and attempts to mislead purchasers about combustible products. Its findings on Arconic, Celotex, and Kingspan show why certificates and marketing claims cannot always be accepted without challenge. When employees or technical specialists know that tested configurations differ from products being marketed, speaking up can become a life-safety control.

Procurement should therefore connect quality reporting to supplier governance. Repeated concessions, unexplained specification changes, waived inspections and rising defect rates deserve comparison with whistleblowing reports and warranty data. Buyers need contractual rights to investigate, obtain technical records and control substitutions where product risk justifies them. A supplier's price and delivery performance cannot compensate for uncertainty about whether the item supplied is the item tested, certified, specified and approved.

Counterfeit Components

Manipulated records are one route to an unsafe product; a substituted component is another. Counterfeit components create a dual deception, since the purchaser believes both that the item is genuine and that its testing, traceability and quality controls apply to it. Risk is highest where components are safety-critical or traded through complex distributor networks. Workers in receiving, maintenance or assembly may be first to notice unusual packaging, inconsistent markings or altered serial numbers.

The UK automotive market provides an example. In July 2025, Trading Standards seized more

than 3,600 counterfeit vehicle parts worth over £100,000 from a South Gloucestershire storage facility, including spark plugs, oil filters and sensors. Intellectual Property Office research reported that one in six surveyed UK motorists had bought counterfeit vehicle parts during the preceding twelve months, often discovering this only after failure or routine servicing. Counterfeiting therefore reaches ordinary safety-critical supply chains.

The problem is not confined to consumer vehicles. In February 2026, the director of UK-based AOG Technics received a sentence of four years and eight months after a £39.3 million aircraft-parts fraud. The Serious Fraud Office found that more than 60,000 engine parts worth £6.9 million were sold with forged airworthiness documentation. Aircraft were grounded internationally after a customer queried authenticity and the manufacturer identified a certificate as fake.

That case demonstrates why employees who know the product may outperform automated assurance. A buyer may see a recognisable part number and accompanying certificate; an engineer may notice that machining, markings, packaging or documentation look wrong. Counterfeit detection therefore benefits from empowering warehouse staff, technicians and maintenance personnel to stop use and escalate concerns without pressure to keep production moving. Quarantine procedures should preserve suspect items and trace every location where equivalent stock has travelled.

Procurement controls should also examine source legitimacy, not merely unit price. Unusually cheap branded parts, unverifiable distributors, broken traceability or sudden changes of source deserve scrutiny, particularly where safety certification matters. In 2023, Border Force seized almost one million counterfeit items worth nearly £200 million overall, while a targeted electrical operation included unsafe hair-styling products and thousands of counterfeit toothbrush heads. Price advantage can disappear instantly when you consider authenticity, recall, and liability risks.

Falsified Testing

Counterfeiting substitutes the product; falsified testing corrupts the proof that a genuine product is safe, which is arguably more dangerous still. A purchaser may reasonably rely on laboratory reports or inspection results when technical verification is beyond its own capability. If sampling is manipulated or results altered, the apparent strength of assurance can conceal greater risk than having no test at all, because decision-makers are positively reassured that standards have been met.

The Grenfell Tower Inquiry found that Celotex's 2014 BS 8414 test incorporated magnesium-oxide boards in critical positions, while the resulting report omitted reference to them. The Inquiry concluded that Celotex subsequently marketed RS5000 using claims derived from that manipulated test. Its wider Phase 2 findings described systematic dishonesty in product testing and marketing. The case demonstrates how seemingly authoritative technical evidence can become unreliable when commercial objectives influence the test itself.

Whistleblowing controls should therefore reach laboratories, quality teams and external testing providers as well as procurement staff. Employees may know that samples were specially prepared, failures repeated until a pass appeared, or reports changed after management intervention. Investigators should secure raw data, sample histories, laboratory communications and version records rather than relying exclusively on the final certificate. Product assurance is strongest when the route from test specimen to marketed product remains independently traceable.

Suppressed Non-Conformities

Falsified tests hide problems before delivery; suppressed non-conformities hide them afterwards. A non-conformity records the gap between what was required and what was actually produced or performed, and suppression occurs when failures are not logged, are downgraded without evidence or hidden from customers to protect delivery targets. The

behaviour can affect dimensions, materials, software or safety features. A low reported defect rate is meaningful only where employees are genuinely permitted to record defects.

Commercial incentives can make suppression attractive. Stopping a production line, scrapping a batch, or notifying a customer may jeopardise margins and delivery performance, while quietly accepting the item may seem cheaper in the short term. Procurement should therefore assess whether quality metrics reward transparency or merely reward low numbers. Sudden reductions in reported defects alongside complaints, returns or warranty claims may justify investigation, particularly where staff report pressure not to create formal non-conformance records.

Grenfell again demonstrates the consequences of disconnect between known product limitations and market representation. The Inquiry's Phase 2 findings concluded that manufacturers manipulated testing and marketing in ways that led purchasers to believe combustible materials complied with relevant guidance. Although the facts are specific and should not be generalised to every quality dispute, they show why adverse technical information must be allowed to travel upwards rather than being managed as an obstacle to sales.

Whistleblowers may be the people who can explain why the quality database looks unexpectedly clean. A technician may know that rejected items were relabelled, a supervisor discouraged defect logging or customer concessions were agreed informally. Investigation should compare reports with scrap, rework, warranty, complaint and production data. The objective is not to penalise honest quality failure; it is to ensure the organisation can distinguish visible failure, which can be corrected, from concealed failure, which cannot.

Whistleblowing Before the Recall

Suppressed non-conformities eventually surface somewhere, and a recall usually marks the point at which the problem becomes publicly visible, though the underlying defect normally existed earlier. Employees may have seen abnormal failure rates, overheating, cracked parts or test anomalies weeks or months before formal escalation. Whistleblowing provides a route around management layers that might otherwise interpret those signals as isolated quality issues, especially where acknowledging a systemic defect would impose substantial replacement and reputational costs.

Current UK data illustrates the volume of corrective activity. During 2025–26, the Product Safety Database recorded 479 recall actions from end users, 249 withdrawals from the market and 611 destruction actions among notified products. These categories are not mutually exclusive and do not represent all unsafe goods, but they show how often product risk requires intervention after distribution has begun. Earlier internal escalation can reduce the population exposed before corrective action starts.

The Office for Product Safety and Standards' 2025–26 report on Haier fridge-freezers provides a practical example of continuing technical scrutiny. Following incidents involving affected models, OPSS investigations identified deterioration of wiring affecting pipework containing flammable refrigerant. The regulator concluded the manufacturer's initial modification solution was unsatisfactory, issued a formal Notice to Warn and required customer contact, after which Haier introduced a revised modification programme. Safety control must remain responsive when first remedies prove inadequate.

Early reporting is valuable because recall economics worsen with scale. A defect identified before mass shipment may require quarantining one production batch; the same defect discovered after national distribution can require customer tracing, public warnings, repairs, refunds, transport and disposal. Although costs vary enormously by product, the commercial incentive to delay disclosure can itself create governance risk. Organisations should therefore separate safety escalation from managers whose performance depends heavily on uninterrupted production or launch dates.

Procurement teams can help by requiring prompt supplier notification of safety incidents, suspected defects, and regulatory contact, rather than waiting for formal recall decisions. Contracts should address traceability, batch identification, access to technical evidence and cooperation during corrective action. Buyers should also monitor whether suppliers repeatedly describe defects as isolated when failure patterns suggest otherwise. Whistleblowing from supplier employees can challenge an optimistic narrative before the buyer receives a formal external notification.

The cultural message should be explicit: reporting a possible defect is not the same as declaring a product unsafe. Employees should be able to raise uncertainty without proving causation. Triage can then combine technical investigation, risk assessment and regulatory advice. A system that demands conclusive evidence before escalation is structurally late; early reporting aims to investigate credible warning signs while the organisation still has opportunities to prevent wider customer exposure.

Environmental Misconduct

The pattern running through product safety repeats in environmental compliance: employees see the gap between documentation and reality before anyone else. Environmental misconduct can involve illegal discharges, waste misdescription, unlawful disposal or falsified records, and employees often see these practices before regulators because they operate treatment plants, transport waste or manage environmental monitoring. In England, the Environment Agency estimates waste crime costs the economy around £1 billion annually.

Southern Water demonstrates the potential financial consequences of sustained environmental offending. In 2021, it received a record £90 million fine after pleading guilty to 6,971 illegal sewage discharges associated with widespread pollution. In July 2026, it was fined a further £7.1 million for separate pollution offences involving incidents between 2019 and 2021. Environmental problems concealed or tolerated operationally can therefore become major criminal, regulatory, financial and reputational events.

Reporting culture matters because environmental wrongdoing can be normalised as an operational shortcut. In the Environment Agency's 2025 waste-crime survey, respondents estimated that only 27% of waste crimes were reported. Whistleblowing channels can help employees disclose instructions to misclassify waste, bypass treatment, falsify sampling or use unlicensed disposal routes. Procurement teams also influence risk by testing whether unusually cheap waste contracts are economically compatible with lawful transport, treatment, tax and disposal.

False Sustainability Claims

Illegal disposal is one environmental risk; exaggerated virtue is another. Sustainability claims increasingly influence purchasing, investment and consumer behaviour, giving organisations commercial incentives to present products or supply chains as greener than the evidence supports. Claims such as sustainable, recyclable, low-carbon or environmentally friendly can mislead when definitions are vague, qualifications are hidden or only favourable lifecycle stages are considered. Procurement teams should require underlying evidence rather than accepting environmental language as assurance in its own right.

The CMA's investigation into ASOS, Boohoo and George at Asda produced formal undertakings in March 2024 requiring clearer and more accurate green claims. Together, the three businesses generated more than £4.4 billion annually from UK fashion sales. The undertakings were given without admission of wrongdoing or liability, an important legal qualification, but the case established detailed expectations concerning fabrics, product ranges, imagery and substantiation that are relevant well beyond those retailers.

The enforcement environment has strengthened since then. Consumer provisions of the Digital Markets, Competition and Consumers Act 2024 took effect in April 2025, allowing the CMA to determine certain consumer-law breaches directly and impose penalties reaching the

higher of £300,000 or 10% of worldwide turnover. Environmental marketing can therefore move beyond reputational criticism into potentially material enforcement exposure where misleading practices fall within the statutory consumer-protection regime.

Advertising enforcement provides further evidence of scrutiny. In December 2025, the Advertising Standards Authority upheld complaints about environmental claims by retailers including Superdry, Nike and Lacoste. In the Superdry ruling, the ASA found that an unqualified “Sustainable Style” claim was ambiguous and unsupported to the required level. Such rulings do not establish criminal wrongdoing, but they show the evidential burden created when broad environmental language outruns the underlying product data.

Whistleblowers can expose the gap between public claims and internal knowledge. Sustainability staff may know that recycled-content figures are estimates, sourcing classifications changed without evidence, or environmental improvements apply only to a limited product subset. Procurement employees may know suppliers cannot substantiate certificates relied upon in marketing. Safe escalation lets organisations correct claims before regulators, customers, or journalists discover that internal evidence contradicts external messaging.

Greenwashing Inside the Supply Chain

A false sustainability claim rarely originates with the brand that makes it publicly. A manufacturer may overstate recycled content, a logistics provider may misrepresent fleet emissions, or a raw-material supplier may provide certificates that cannot be traced to actual production. The buying organisation can then repeat inaccurate information innocently but still face consequences. Supply-chain assurance must therefore test the provenance of claims instead of treating supplier declarations as transferable proof.

The CMA’s fashion-sector work illustrates why specificity matters. Its undertakings with ASOS, Boohoo and George at Asda required environmental statements about materials to be specific and clear rather than relying on broad words such as “eco”, “responsible” or “sustainable” without adequate explanation. Those requirements targeted retailers, but the evidence needed to support such claims often originates with upstream manufacturers, fibre producers, certification schemes, and logistics providers.

Commercial pressure can worsen the problem. Suppliers know that sustainability credentials increasingly affect tender scores and market access, creating incentives to present incomplete evidence optimistically. Buyers should therefore separate ambition from verified performance, require traceable methodologies and challenge sudden environmental improvements unsupported by operational change. A supplier moving from 30% to 80% recycled content should demonstrate the material flows, certification and production records supporting that result rather than merely revising a questionnaire response.

Employees inside the supply chain may know that the documentation tells only part of the story. They may see virgin material substituted for recycled input, certified feedstock mixed with unknown sources or environmental labels applied across product ranges despite limited qualifying production. Whistleblowing gives buyers access to contradictory evidence that routine assurance might never request. The appropriate response is careful investigation and correction, not assuming either the supplier declaration or allegation is automatically true.

Carbon and Environmental Data Manipulation

Beyond marketing language, the underlying numbers themselves can be manipulated. Environmental reporting increasingly depends on data gathered from suppliers, facilities, meters and modelling assumptions, and manipulation can involve changing boundaries, omitting high-emission sites, selecting favourable factors or reporting estimated values as measured results. Not every error is dishonest; carbon accounting involves judgement and evolving methodologies. Governance should nevertheless distinguish legitimate estimation uncertainty from deliberate choices designed to flatter performance.

Drax provides a significant UK example of inaccurate sustainability reporting. Ofgem's investigation found that Drax misreported certain biomass profiling data. However, it found no evidence that Drax failed the sustainability threshold for receiving Renewables Obligation support or that certificates were issued incorrectly. Drax made a £25 million payment into Ofgem's Voluntary Redress Fund and was required to commission extensive independent assurance over its supply-chain profiling data.

The financial context demonstrates why data quality matters. Ofgem recorded that Drax received 9,279,992 Renewables Obligation Certificates for 2023–24, valued at an estimated £548 million. The regulator emphasised that the identified profiling errors were technical and did not affect subsidy entitlement, so it would be inaccurate to describe the case as subsidy fraud. It nevertheless required stronger governance because environmental datasets inform policy, statistics, public scrutiny and confidence in support schemes.

The case also illustrates how assurance can reach deep into a supply chain. Ofgem required an independent audit covering 98% of Drax's global supply chain for the relevant profiling data and reasonable assurance over reporting. That scale is important because carbon and sustainability metrics often aggregate thousands of underlying transactions. A board-level number can look precise while depending on supplier classifications, sampling, source documentation and manual judgments made far from headquarters.

Whistleblowers can identify manipulations that assurance sampling misses. An employee may know that a facility deliberately excluded a meter, that supplier emissions were replaced with a favourable default or that adverse environmental incidents were omitted from a sustainability dataset. Investigators should preserve source data and calculation histories so they can reconstruct reported metrics. Version control is particularly important where spreadsheet models or manual adjustments materially influence externally reported performance.

Boards should also guard against target-driven reporting cultures. Net-zero commitments, sustainability-linked finance and executive incentives can make environmental indicators commercially consequential. The stronger the reward for meeting a target, the stronger the need for independent challenge around measurement. Good controls define methodologies before results are known, record changes transparently and ensure technical employees can raise concerns safely without being characterised as obstructing strategic environmental ambitions.

Whistleblowing and ESG Assurance

The common thread across labour, safety, product and environmental risk converges here: ESG assurance is strongest when quantitative reporting is tested against human intelligence. Supplier questionnaires, certificates, audit reports and carbon datasets describe what organisations say is happening; workers may know what actually happens between audit visits. Updated Home Office modern-slavery guidance warns that audits should not be relied upon alone and recommends worker-centred practices, a principle that applies equally to environmental, safety and governance assurance.

Whistleblowing does not replace professional assurance. Reports can be mistaken, incomplete or motivated by workplace disputes, while auditors can test samples systematically and assess controls against defined criteria. The advantage comes from combining both. A worker allegation can direct assurance toward an unreported subcontractor, manipulated test, or false environmental dataset; audit evidence can then confirm, qualify, or disprove the concern. Human intelligence makes self-reported supplier information challengeable rather than self-authenticating.

Boards should therefore ask whether ESG reporting systems can absorb contradictory evidence. A mature process links disclosures with modern-slavery assessments, safety incidents, product complaints, environmental data, supplier audits and risk registers, then tracks remediation to completion. If whistleblowing sits in HR while ESG reporting sits elsewhere, serious intelligence may never affect published claims. Assurance becomes

credible when inconvenient information can travel from the worker or supplier floor to those signing the organisation's public statements.

Falsification of Supplier Performance Data

If assurance is strongest when tested against human intelligence, ordinary contract data deserves the same scepticism. Supplier performance data can mislead when reported KPIs are altered, exclusions are stretched, incidents are reclassified or failures disappear before reaching the customer. The danger is greater where payment, service credits, renewal or executive bonuses depend on measured performance. A dashboard may appear objective while reflecting choices the supplier made about what counts and when the clock starts.

The Ministry of Justice's electronic-monitoring contracts illustrate why customer verification matters. A 2013 National Audit Office review recorded disputed charging for periods when monitoring equipment had been removed, when installation had never succeeded and, in some cases, multiple charges for one individual subject to concurrent orders. PwC estimated potential overcharging by G4S and Serco in the tens of millions of pounds, although contractual interpretation was disputed at the time.

Later proceedings exposed a different form of distorted reporting. Serco Geografix entered a deferred prosecution agreement after accounting manipulation artificially reduced profit margins reported to the Ministry of Justice; the resolution involved a £19.2 million penalty and £70 million compensation. G4S Care and Justice Services subsequently paid a £38.5 million penalty after false information concerning electronic-monitoring costs, alongside a previous £121.3 million civil settlement with the Ministry.

Buyers should therefore test performance information against source records rather than accepting supplier-produced dashboards as complete assurance. Useful checks include raw transaction data, timestamped service logs, customer complaints, system telemetry, invoice records and independent sampling. Whistleblowers add another layer because employees may know which failures were recategorised, which data fields were manually altered or which apparent improvements resulted from changing measurement rules rather than improving the underlying service.

False Certifications and Audit Evidence

Distorted KPIs corrupt performance data; false certification corrupts the documents behind it. Certificates provide efficiency because buyers cannot retest every component, inspect every workplace or reproduce every specialist assessment, but that efficiency creates dependency on the authenticity and scope of the documents supplied. False accreditation, forged inspection evidence or certificates applied beyond the product actually tested can transform assurance into deception. Procurement teams should understand what a certificate proves and who issued it.

Verification should therefore go beyond checking that a PDF exists. Buyers can confirm accreditation directly with issuing bodies, validate certificate numbers, check expiry and scope, compare product identifiers and retain evidence of verification. High-risk goods may justify independent testing or witnessed inspection. Where certificates are supplied repeatedly, procurement systems should flag sudden issuing-body changes, inconsistent document formats, or identical reports appearing across different batches, factories, or suppliers without a plausible explanation.

Whistleblowing is particularly valuable where documentation looks flawless. A laboratory technician may know that samples were substituted; a quality manager may know that an expired certificate was altered; a distributor may know that supporting documents were copied from genuine stock. Such reports should trigger controlled verification rather than immediate accusation. The central lesson is that certification reduces information asymmetry only when the underlying evidence, issuer and chain of custody remain trustworthy.

Social Audit Manipulation

Documents can be falsified; so, just as easily, can the audits meant to catch them. Social audits can identify labour abuses, but they remain snapshots taken in environments suppliers may have prepared for inspection. Updated Home Office guidance warns that modern slavery may remain hidden because suppliers can present fake records and coach workers to tell auditors that conditions are better than they are. An immaculate audit cannot be treated as conclusive evidence of genuinely lawful conditions.

Audit design should make manipulation harder. Government guidance recommends independent specialists trained in forced-labour indicators and recognises the value of unannounced inspection. PPN 009 model clauses go further by allowing authorities, where appropriate, to conduct unannounced or semi-announced site inspections and speak directly with supplier employees confidentially and in their native language. These measures reduce management's ability to select interviewees, script responses or temporarily improve visible conditions before inspectors arrive.

Worker voice provides the counterfactual against which staged assurance can be tested. Employees can explain whether records shown to auditors match actual hours, whether recruitment debts exist or whether supervisors instructed them what to say. Reporting channels should therefore remain available between audits and outside management control. An audit that records no findings while confidential worker reports consistently describe exploitation is not reassurance; it is evidence that the assurance method itself requires scrutiny.

Gaming Service-Level Agreements

Staged audits manipulate one assurance mechanism; gamed service levels manipulate another. Service-level agreements improve performance only if their measures reflect outcomes that matter, and gaming occurs when suppliers optimise the measurement rather than the service: tickets are closed and reopened to reset clocks, difficult cases are excluded or resources concentrate narrowly on measured activity while unmeasured quality deteriorates. The supplier may technically meet the target while customers experience worsening service.

Measurement design therefore matters as much as the numerical threshold. A 95% response target can conceal serious failure if the remaining 5% includes the highest-risk cases, while an average resolution time can improve even as a small group waits exceptionally long. Buyers should examine distributions, exceptions, repeat incidents and customer outcomes alongside headline KPIs. Service credits should not inadvertently reward suppliers for redefining failure or discourage transparent reporting of difficult cases.

Electronic monitoring offers a current example of why headline compliance needs context. The National Audit Office reported in 2026 that Serco met its 95% timeliness target for tag-fitting visits in February, yet tags were fitted to only 62% of individuals on the first attempt. The figures measure different things, but that is precisely the governance lesson: a supplier can meet a contractual activity target while the wider service outcome remains materially weaker.

Gaming may also occur around denominator management. Cases judged outside scope, paused while awaiting customer information or transferred between queues can disappear from reported breaches depending on contract definitions. Some exclusions are legitimate, so procurement teams should examine changes over time rather than assume manipulation. Sudden performance improvement following classification changes deserves explanation, especially where complaints, backlogs or operational incidents do not show equivalent improvement.

Contracts should give customers access to definitions, calculation methods and underlying data sufficient to reproduce material KPIs. Change control should govern amendments to measurement rules, and audit rights should include source systems where proportionate. Independent assurance becomes especially useful where substantial service credits, gainshare or renewal decisions depend on supplier-reported performance. The key question

is whether improved scores correspond with improved outcomes rather than simply more advantageous interpretation of the measurement framework.

Whistleblowers can identify deliberate gaming before statistical review does. Employees may know that managers instruct teams to close tickets prematurely, avoid logging failures or prioritise cases solely because they fall inside a measured category. Reporting mechanisms should distinguish genuine disagreement over SLA interpretation from intentional misrepresentation. Where manipulation is substantiated, remediation should correct historical reporting, financial consequences and measurement design rather than merely disciplining the individual who changed the data.

Whistleblowing as a Counterweight to Self-Reporting

Supplier assurance inevitably relies partly on self-reporting because customers cannot observe every transaction, workplace or system continuously. Questionnaires, KPI packs, modern-slavery statements, cyber assessments and environmental datasets therefore depend on information generated by organisations whose commercial interests may favour positive results. Most suppliers report honestly, but the structural conflict remains. Whistleblowing provides a counterweight by allowing people inside the supplier to challenge the official account when operational reality differs materially from reported assurance.

Cybersecurity demonstrates the scale of the gap. The 2025–26 Cyber Security Breaches Survey found that only 15% of UK businesses formally reviewed cyber risks presented by immediate suppliers and just 6% reviewed their wider supply chains. Even among large businesses, the figures were 48% and 24%, respectively. Self-assessment can help prioritise scarce resources, but limited external review makes credible internal reporting from supplier personnel particularly valuable when declared controls are not operating in practice.

Assurance should therefore be triangulated. Compare supplier statements with incident records, customer complaints, audit findings, certification databases, system telemetry, worker interviews, and protected disclosures. Contradiction does not automatically mean dishonesty; methodologies differ, and reporters can be mistaken. It does mean the buyer should investigate rather than resolve the inconsistency by defaulting to the supplier's formal submission. Self-reporting becomes trustworthy when it is challengeable, evidenced and capable of correction.

Cybersecurity Failures

Supplier personnel may discover vulnerabilities before customers because they configure systems, review logs, administer patches and respond to incidents. A customer can receive a clean assurance questionnaire while engineers inside the supplier know that multi-factor authentication is incomplete, unsupported software remains exposed, or vulnerability scans have repeatedly failed. Cyber assurance therefore requires channels that let concerns reach people who can act, even when commercial managers prefer not to disrupt delivery or disclose weakness.

The UK threat environment makes that visibility important. The 2025–26 Cyber Security Breaches Survey found that 43% of businesses identified a cyber breach or attack during the preceding twelve months, equivalent to approximately 612,000 businesses. The rate rose to 65% among medium and 69% among large businesses. These figures capture only identified and reported incidents, meaning hidden or undetected compromises may make actual exposure higher than the survey can measure.

Advanced Computer Software provides a supplier-side case study. The ICO fined the business £3.07 million in March 2025 after a 2022 ransomware attack affected systems used by NHS and healthcare customers. The attack exposed personal information relating to 79,404 people, including details about gaining entry to the homes of 890 people receiving home care. The ICO identified weaknesses including incomplete multi-factor authentication, inadequate patch management and insufficient vulnerability scanning.

NCSC guidance accordingly recommends ongoing supplier security monitoring rather than a one-off assessment. Buyers can require measurable security obligations, vulnerability information, incident-reporting procedures, penetration testing and evidence that agreed controls continue operating. The NCSC also asks whether suppliers encourage users to report suspected or actual incidents promptly in a no-blame environment. That cultural question matters because sophisticated technical controls can still fail when employees believe raising weaknesses will damage careers or customer relationships.

Contracts should identify which supplier systems, subcontractors and privileged users can affect the customer's critical assets. Controls can then be proportionate to consequence rather than imposed uniformly. A supplier hosting public information does not necessarily require the same scrutiny as one processing health records or administering production networks. Risk ownership nevertheless remains with the customer organisation, even where third parties implement controls, a point emphasised in NCSC risk-management guidance.

Concealed Data Breaches

Pressure to conceal a data breach can arise from fear of regulatory action, reputational damage, customer claims or contractual penalties. Delay is dangerous because customers may need to contain the compromise, warn individuals or meet their own legal deadlines. Under UK GDPR, a controller must notify the ICO of a notifiable personal-data breach without undue delay and, where feasible, within 72 hours of becoming aware of it. Waiting for complete certainty can therefore create compliance risk.

Processors have a different but connected duty. ICO guidance states that a processor must inform the controller without undue delay after becoming aware of a personal-data breach, allowing the controller to decide whether ICO notification is required. Article 28 contracts should address this reporting obligation. Government's 2026 model action plan recommends even tighter contractual service levels for departments, suggesting third-party processors should report suspected personal-data breaches within 12 to 24 hours of discovery.

Concealment can be subtle. A supplier may describe exfiltration as a routine security incident, delay escalation while forensic work continues or avoid confirming that customer information was involved. Investigators should distinguish genuine uncertainty from deliberate suppression; cyber incidents are often technically complex and early facts change. The governance requirement is prompt disclosure of known material facts and uncertainty, not instant certainty about the full scale, cause, and consequences of an attack.

Capita's 2023 cyber attack shows how quickly a supplier-side compromise can become a major data event. In October 2025, the ICO imposed combined penalties of £14 million after hackers accessed information relating to more than six million people. The attack began when a malicious file was downloaded to an employee device; although a high-priority alert appeared within ten minutes, the affected device was not quarantined for 58 hours.

Whistleblowers can be decisive when formal incident channels stall. Security analysts may know that data left the network, customer records were affected, or senior managers have instructed teams to minimise written references. Protected reporting should route such concerns quickly to independent security, legal or board oversight without encouraging employees to extract additional confidential data themselves. The reporter's task is to raise credible information, not to conduct unauthorised forensic investigation or prove regulatory breach.

Customers should contract for notification thresholds that are clearer and faster than legal minimums where operational dependency justifies it. Requirements can cover suspected incidents, confirmed breaches, material vulnerabilities, ransomware and subcontractor events, with staged updates as facts develop. Concealment then becomes both a governance and contractual issue. Prompt reporting may be uncomfortable, but delayed disclosure can expand technical harm while reducing the time available to protect customers, regulators and affected individuals.

Inappropriate System Access

Privileged accounts can create disproportionate risk because administrators may access data, alter configurations, create users and suppress logs unavailable to ordinary staff. Supplier personnel sometimes receive broad permissions to support customer environments, making identity governance a procurement concern as well as an IT issue. Access should follow least-privilege principles, be attributable to named individuals and expire when no longer required. Shared administrator accounts weaken accountability because subsequent investigation cannot establish who performed a particular action.

The 2025–26 Cyber Security Breaches Survey found that 6% of large UK businesses reported unauthorised access to files or networks by staff, even if accidental, compared with 1% of businesses overall. 3% of large businesses reported external unauthorised access. These figures are based on incidents organisations identified, but they demonstrate that inappropriate access is not purely theoretical and that larger organisations encounter insider and external access problems in practice.

Controls should combine identity management with behavioural evidence. Multi-factor authentication, privileged-access management, time-limited elevation, session logging and regular entitlement reviews reduce opportunity, while alerts can identify unusual downloads or out-of-hours administration. Suppliers should also remove accounts promptly when staff change roles or leave. A quarterly spreadsheet certifying that access is correct provides limited assurance if the underlying system still contains dormant privileged accounts created years earlier.

Whistleblowing adds context that logs cannot. Colleagues may know that an administrator routinely accesses customer records out of curiosity, shares credentials or grants emergency rights without approval. The NCSC specifically encourages supplier assessment to consider insider threat and whether users can report suspected incidents promptly in a no-blame environment. Reports should be tested against access records, not assumed true, but they can direct investigators towards activity ordinary monitoring has not prioritised.

Third-Party Cyber Risk

Third-party cyber risk expands as organisations outsource hosting, payroll, software, logistics, professional services and operational technology. Each connection can introduce credentials, data stores, remote access or software dependencies outside the customer's direct control. NCSC guidance stresses that supply-chain vulnerabilities may be inherent, introduced or exploited at any point. The challenge is therefore not simply whether the immediate supplier is secure, but whether the wider delivery ecosystem contains a route into critical information or services.

The 2025–26 Cyber Security Breaches Survey exposes a continuing assurance gap. Only 15% of businesses formally reviewed risks posed by immediate suppliers, and 6% examined the wider supply chain. Among large businesses, where capability is generally stronger, 48% reviewed immediate suppliers but only 24% reviewed the wider chain. Just 11% of businesses required suppliers to hold any cybersecurity standard or accreditation, showing how limited formal supplier requirements remain across much of the economy.

The 2024 Synnovis ransomware attack demonstrates operational dependency. Synnovis provides pathology services to NHS organisations, and the attack significantly reduced testing capacity. NHS England later reported delays affecting more than 11,000 outpatient and elective appointments, while stolen data potentially related to service users beyond the most affected south-east London trusts. A cyber incident at one supplier therefore disrupted clinical pathways across organisations that were not themselves the original attack target.

Supplier mapping should identify subcontractors, software components, hosting providers, and other dependencies that could affect critical services. NCSC's Cyber Assessment Framework treats limited visibility of subcontractors and unrestricted or unmonitored supplier

access as indicators of weak supply-chain security. Mapping does not eliminate risk, but it establishes where contractual controls, assurance, contingency planning and incident notification are needed instead of discovering critical fourth-party dependencies only after disruption occurs.

Concentration adds another dimension. Several customers may depend on the same software platform, cloud environment or managed-service provider, creating correlated failure even when each buyer individually diversified its direct suppliers. Procurement should therefore consider systemic dependency, exit feasibility and recovery arrangements alongside conventional supplier financial health. A low-cost vendor can become a high-impact concentration risk when compromise simultaneously affects hundreds of organisations using identical infrastructure, credentials or update mechanisms.

Whistleblowing provides intelligence from inside those interconnected chains. An engineer at a subcontracted hosting provider may know that customer environments are inadequately segregated; a software developer may know a critical library is unsupported. Buyers cannot rely on contracts alone to reveal such facts. Effective supplier assurance combines contractual duties, technical monitoring, independent assessment and safe human reporting so that information can cross organisational boundaries before a hidden vulnerability becomes a shared incident.

Reporting Technology Misuse

Technology misuse often becomes visible first to colleagues, not automated controls. Employees may see privileged accounts used for personal searches, customer data exported without justification, security tools disabled or monitoring capabilities redirected towards inappropriate targets. These observations can reveal conduct that generates no obvious external alarm. A mature cyber programme therefore treats internal reporting as part of detection architecture, alongside logging, endpoint monitoring, access reviews and automated anomaly detection.

The NCSC encourages organisations to create clear vulnerability-disclosure processes because people who discover security weaknesses need a safe route to report them. Its guidance stresses that reports can provide valuable information and recommends validation, triage and feedback to the finder. The same principle applies internally: staff who discover misuse need a route that reaches security personnel who can preserve evidence without requiring the reporter to confront the person whose access is being questioned.

Reports should distinguish misuse from authorised but unfamiliar activity. Security administrators legitimately perform actions that would appear suspicious in most roles, while emergency response sometimes requires unusual access. Investigation should therefore combine the allegation with identity logs, change records, approvals and system telemetry. This protects against both unchecked misuse and false accusations. Reporting channels work best when staff are encouraged to describe observed facts, dates and systems rather than speculate about criminal motive.

Customers should ask whether important suppliers foster that reporting culture. NCSC supplier-assurance questions explicitly ask whether users are encouraged to report suspected or actual security incidents promptly in a no-blame environment and whether the supplier has assessed insider threat. Those questions move assurance beyond firewalls and certifications towards organisational behaviour. A supplier may have sophisticated tooling yet remain vulnerable if employees believe raising misuse will be ignored, punished, or treated as disloyalty.

The Supplier's Employees as a Source of Assurance

Supplier employees possess operational knowledge that buyers cannot recreate through periodic audits. They know whether procedures are followed when auditors leave, whether shortages are concealed, whether subcontractors are approved and whether reported KPIs

reflect actual delivery. This does not make every employee allegation reliable, but it makes employees an important source of assurance. Formal reporting from management describes the control environment; workers can reveal whether that environment operates consistently in practice.

Modern-slavery guidance increasingly recognises that distinction. The Home Office's current transparency guidance recommends multiple reporting channels for workers, including people employed within supply chains, and says anonymous mechanisms should be available in languages workers understand. It also explains that stakeholder engagement can help organisations identify higher-risk areas and understand whether prevention or remediation is working. Worker information is therefore not merely grievance handling; it can materially improve supply-chain due diligence.

Cybersecurity presents the same logic. Engineers inside a supplier can know that patches are delayed, administrator accounts are shared, or security alerts are routinely suppressed long before the customer's annual assessment discovers anything. Product technicians may know of substituted materials; warehouse staff may recognise counterfeit stock. Assurance improves when buyers deliberately create routes through which such operational knowledge can challenge supplier-generated evidence without assuming that bypassing supplier management should become routine.

The relationship requires care because supplier employees owe duties to their own employer and may handle confidential information. Buyers should not encourage unauthorised extraction of documents, hacking or breaches of legal privilege. ACAS guidance makes clear that whistleblowers are not responsible for gathering evidence and may create legal problems by taking information improperly. A reporting mechanism should therefore invite descriptions of concerns and legitimately held evidence, leaving investigation to authorised teams and regulators.

The strongest model combines supplier management information, audits, analytics and worker voice. Each source compensates for weaknesses in the others: management understands systems, auditors provide structured testing, data reveals patterns and employees contribute lived operational knowledge. Contradictions should prompt inquiry rather than automatic preference for one source. The objective is not to turn supplier workforces into informants, but to prevent commercial hierarchy from becoming the only route through which customers learn about serious risk.

Should Buyers Provide External Speak-Up Channels?

For higher-risk supply chains, buyers should consider allowing supplier employees to raise serious concerns directly, especially where allegations involve the supplier's management or the customer's contract. Current Home Office guidance recommends multiple channels through which workers, including those in supply chains, can report concerns anonymously and in languages they understand. PPN 009 also asks whether effective whistleblowing or grievance mechanisms exist for workers and supply-chain workers delivering government contracts.

The channel should be proportionate, not universal by default. A direct reporting route is most valuable where contracts involve vulnerable workers, critical infrastructure, safety-sensitive products, substantial public money or material cyber access. Buyers must also decide who receives reports, how conflicts are managed and when the supplier is informed. Creating a hotline without investigative capacity, confidentiality controls or remediation authority can raise expectations the buyer is not equipped to meet.

Legal protection requires careful explanation. A supplier employee who reports to a customer may sometimes make a protected disclosure if they reasonably believe the customer or another recipient is responsible for the wrongdoing, but statutory protection depends on the Employment Rights Act conditions and facts. An external buyer channel should therefore never promise automatic legal protection. It should explain confidentiality limits, permitted

escalation and access to independent advice while contractually prohibiting retaliation where possible.

Protecting Supplier Whistleblowers

Protecting a supplier whistleblower is harder because the buyer does not control the reporter's employment relationship, workplace or line management. The buyer can preserve confidentiality, restrict disclosure, investigate proportionately and impose contractual expectations, but it cannot guarantee that retaliation will never occur. Procurement documents should therefore avoid promises beyond the buyer's control. Protection begins with minimising unnecessary identification and considering retaliation risk before sharing information back with the supplier.

UK whistleblowing law may still assist some supplier employees. Acas explains that a worker can make a protected disclosure to someone other than their employer where they reasonably believe that person is responsible for the wrongdoing. Protection depends on the requirements, including reasonable belief and public interest, and other external disclosures face additional tests. A buyer should therefore signpost legal or regulatory routes rather than presenting its contractual hotline as a substitute for statutory advice.

Contractual protections can nevertheless be meaningful. Buyers can require suppliers not to retaliate against workers who raise concerns in good faith, to preserve employment records relevant to an allegation, to cooperate with investigations, and to provide evidence of remediation. Serious retaliation can itself become a contract-management issue. Draft clauses carefully because the customer cannot rewrite employment law or control every management decision, but commercial leverage can reinforce standards that legal remedies alone may not prevent.

Practical protection also requires communication. A supplier should not automatically receive the reporter's name merely because it employs them, and investigators should consider whether they can test facts without revealing identity. When disclosure is necessary for fairness or legal reasons, the reporter should be told, where possible. Anonymity is not always sustainable, particularly in small teams where circumstances identify the source, making anti-retaliation monitoring and follow-up as important as initial confidentiality.

Supplier Codes of Conduct

Supplier codes of conduct turn broad organisational values into explicit expectations for businesses seeking or performing contracts. Effective codes should address bribery, conflicts, labour standards, modern slavery, environmental conduct, data security and speaking up, while distinguishing mandatory contractual obligations from aspirational principles. A code that merely restates values without consequences can become reputational decoration. Its value lies in setting standards that procurement can test during selection, mobilisation, contract management and renewal.

The UK Government Supplier Code of Conduct provides a useful benchmark. It states that suppliers are expected to maintain a comprehensive whistleblowing policy that allows employees to report incidents or concerns anonymously, safely, and without repercussion. The Code also covers conflicts, confidentiality, cyber security, tax, social value and employment standards. Although its precise legal effect depends on contractual incorporation and procurement context, it demonstrates that whistleblowing expectations can form part of mainstream supplier governance.

Codes should explain scope clearly. Employees need to know whether they can report concerns about their own employer, subcontractors, customer personnel or conduct affecting the contract. Suppliers should know whether anonymous reporting is accepted, what serious matters must be escalated to the buyer and what records must be retained. Ambiguity encourages inconsistent treatment. A short code supported by detailed procedures is often stronger than a lengthy document whose reporting expectations disappear among dozens of

commitments.

Test implementation rather than assume it. Buyers can ask suppliers to provide evidence of training, reporting routes, investigation governance, board oversight, and anonymised case data appropriate to risk. A supplier saying it has a whistleblowing policy answers only the first question. Assurance should examine whether workers know the channel, whether reports reach independent decision-makers and whether retaliation allegations are tracked. Zero reports over many years may justify cultural enquiry rather than automatic praise.

Codes should also account for legal and cultural differences across international supply chains. Anonymous hotlines may be unfamiliar, local labour protections vary, and workers may distrust channels operated from another country. Suppliers should provide accessible routes in relevant languages and formats while respecting local law. Where modern-slavery risk is material, worker representatives, trade unions or specialist organisations may provide trusted alternatives that make a formal code meaningful beyond corporate headquarters.

Consequences need proportionality. Minor failure to display a hotline poster should not automatically trigger termination, while concealed forced labour, bribery or serious retaliation may justify urgent escalation. Contracts can link codes to corrective-action plans, audit rights, suspension, removal of individuals or termination depending on severity. The objective is to create leverage for improvement and accountability, not to produce automatic disengagement that may harm workers or destroy evidence before underlying problems are understood.

Building Speak-Up Obligations into Contracts

Contracts can convert speak-up expectations from voluntary aspiration into defined supplier responsibilities. Appropriate clauses may require a reporting mechanism, confidentiality safeguards, non-retaliation, investigation arrangements, record retention and cooperation with customer enquiries. Requirements should reflect contract risk rather than imposing identical machinery on every small supplier. The purpose is to ensure serious concerns about delivery can travel safely beyond ordinary management lines, particularly where the supplier handles vulnerable people, critical systems or substantial public expenditure.

PPN 009 provides a concrete public-sector model in the modern-slavery context. Its example clauses require suppliers to maintain relevant policies and due diligence, extend anti-slavery provisions into subcontracting and report discovery or suspicion of slavery, trafficking, forced labour or child labour to the authority and relevant bodies. Optional provisions support unannounced inspections, confidential worker interviews and subcontractor audits. Private-sector buyers can adopt equivalent clauses voluntarily, without the statutory trigger applying to central government.

Drafting should define thresholds carefully. Requiring notification of every employee grievance may overwhelm both parties, while limiting reporting to proven illegality creates a threshold too high for early warning. Contracts can distinguish urgent matters—such as suspected bribery, serious safety incidents, material cyber breaches or modern slavery—from periodic thematic reporting. They should also specify timescales, recipients, confidentiality expectations and whether oral notification must be followed by written information.

Contract clauses cannot substitute for culture. A supplier may technically maintain a hotline while workers fear using it, or report incidents contractually while discouraging internal escalation. Contract management should therefore test effectiveness through worker awareness, sample cases, audit findings and retaliation monitoring where proportionate. Speak-up obligations work best when tied to governance, assurance and remediation rather than treated as another warranty checked once at mobilisation and ignored until the contract expires.

Supplier Notification Duties

Supplier notification duties determine when information must move from the supplier's internal governance into the customer relationship. Appropriate triggers can include serious safety

incidents, material service failures, cyber events, suspected bribery, regulatory investigations, modern-slavery concerns or circumstances threatening continuity. The duty should focus on matters relevant to the customer and the contract rather than requiring disclosure of every internal issue. Overbroad clauses generate noise; excessively narrow clauses create incentives to delay disclosure until facts are incontrovertible.

Cyber contracts illustrate why timing matters. ICO guidance requires processors to inform controllers without undue delay after becoming aware of a personal-data breach. The Government's 2026 model breach-response plan recommends departmental contracts go further, using service levels that require third-party processors to notify suspected breaches within 12 to 24 hours. Earlier contractual notification gives controllers more time to investigate and, where required, meet the UK GDPR's 72-hour deadline for notifying the ICO.

Security obligations can extend beyond personal data. Government call-off terms provide examples requiring parties to notify one another when they become aware of actual, potential or attempted security breaches and requiring suppliers to take reasonable steps to minimise harm and remedy the breach. Such provisions recognise that a customer may need to act before the supplier understands the full incident. Staged notification allows early warning followed by progressively more complete technical information.

Modern-slavery guidance uses a similar principle. PPN 009 model clauses require suppliers to report discovery or suspicion of slavery, trafficking, forced labour, child labour, involuntary prison labour or labour-rights abuse by themselves or subcontractors to the authority and relevant bodies. Importantly, the trigger is suspicion or discovery, not final proof. This supports early safeguarding and investigation while avoiding the impossible expectation that supplier managers establish criminal liability before telling the customer.

Notification should not become an incentive for concealment through punitive automatic consequences. If every reported incident immediately produces termination or severe service credits, suppliers may rationally dispute classification and delay escalation. Contracts should reserve strong remedies for serious conduct while recognising prompt self-reporting, cooperation and remediation as relevant factors. The Serco electronic-monitoring DPA itself illustrates the broader enforcement principle: prompt voluntary self-disclosure and substantial remediation were factors considered in agreeing the resolution.

Governance should track notification performance separately from incident frequency. Useful measures include whether reports were timely, sufficiently complete, updated as facts changed and followed by corrective action. A supplier experiencing incidents but reporting them promptly may present stronger governance than one claiming none while external sources reveal problems. Whistleblowing can test that picture by giving employees a route to report customer-relevant events they believe management has improperly withheld or minimised.

Pass-Through Requirements

Pass-through clauses extend selected obligations from the prime supplier to subcontractors whose conduct can affect contract outcomes, particularly where labour, cybersecurity, safety or data processing occurs below Tier One. PPN 009 model clauses require suppliers to include anti-slavery provisions in subcontracting and undertake due diligence across relevant supply chains. Private-sector contracts can mirror this discipline through equivalent flow-down clauses without a government trigger. Without pass-through, standards at Tier One rarely survive contact with lower tiers.

Pass-through should be targeted, not indiscriminate. Relevant requirements might cover confidentiality, incident notification, worker reporting, security controls, modern-slavery standards, audit cooperation and retention of evidence. The prime supplier should remain accountable for managing its subcontractors rather than turning the customer into the direct manager of every lower-tier relationship. Contract terms should also require visibility of material subcontracting changes so the buyer knows where critical services, data or

vulnerable workers have moved.

Speak-up access should travel with those obligations. A subcontractor worker who sees exploitation, falsified records or concealed cyber incidents needs to know how concerns can reach an independent recipient. Contracts can require suppliers to communicate reporting channels down the chain and prohibit retaliation, while recognising that legal protection depends on employment and whistleblowing law. The result is stronger assurance: obligations do not merely cascade on paper; compliance information can travel back up.

Audit Rights

Audit rights matter because contractual promises are valuable only if the buyer can test whether they operate in practice. A supplier may maintain policies, hotlines and training records while employees remain unaware of them or fear using them. Proportionate audit clauses can permit document review, interviews, system sampling and inspection of relevant subcontractor arrangements, allowing the customer to compare stated controls with operational evidence rather than relying exclusively on annual declarations.

Cybersecurity guidance illustrates the principle. The National Cyber Security Centre asks buyers to consider contractual rights to audit suppliers and, where relevant, require equivalent rights over subcontractors. It also recommends ongoing monitoring rather than one-off assessment, including security KPIs, breach information, privileged-access controls and assurance over suppliers further down the chain. Audit rights therefore work best when they support continuous risk management rather than an occasional compliance exercise performed immediately before contract renewal.

Modern-slavery assurance requires similar flexibility. PPN 009 provides model provisions supporting unannounced or semi-announced inspections, confidential conversations with workers in their own language and audits of subcontractors where proportionate. Those powers are significant because staged site visits can hide abusive conditions. A contractual right exercised only through management-selected documents and scheduled interviews may confirm that procedures exist without establishing whether vulnerable workers can report concerns safely.

Audit rights should nevertheless remain bounded. Customers need a legitimate purpose, appropriate confidentiality protections and safeguards for personal, commercially sensitive and privileged information. Unlimited access can create its own security, data-protection, and operational risks. The stronger model defines scope, notice, evidence, access conditions, remediation and escalation in advance, while preserving enhanced or urgent rights where credible allegations suggest serious wrongdoing that ordinary assurance cannot resolve.

Non-Retaliation Commitments

Non-retaliation clauses express a simple commercial expectation: nobody should be disadvantaged for raising a genuine concern in good faith or providing information to an authorised investigation. Contract wording can prohibit dismissal, demotion, intimidation, loss of work, blacklisting or other adverse treatment linked to reporting. Such commitments matter particularly where the reporter works for a supplier, because the buyer may influence contract consequences while lacking direct control over employment decisions inside another organisation.

The UK Government Supplier Code of Conduct expects suppliers to maintain comprehensive whistleblowing policies that allow employees to report concerns anonymously, safely, and without repercussion. It also expects suppliers to speak out when government behaviour, governance or contractual arrangements create serious problems. That reciprocal expectation is important: ethical supply relationships require challenge to flow in both directions, rather than treating whistleblowing solely as a mechanism through which customers scrutinise suppliers.

Contractual protection does not create statutory whistleblowing rights where legislation does

not provide them. Acas notes that some people, including genuinely self-employed individuals, volunteers without enforceable employment contracts and non-executive directors, are generally outside Great Britain's statutory whistleblowing protection even though an organisation may voluntarily accept reports from them. A supplier code can therefore promise fair treatment and contractual consequences for retaliation, but it should not misrepresent the legal remedies available to every reporter.

Non-retaliation should be measurable, not rhetorical. Buyers can require suppliers to record retaliation allegations, investigate them separately from the underlying disclosure and report material findings appropriately. Contract managers should also watch indirect indicators: removal from projects, unexplained shift changes, denied overtime, disciplinary action or termination soon after reporting. None automatically proves retaliation, but temporal patterns deserve examination when a worker who raised a serious concern subsequently suffers adverse treatment.

Remedies should target both the individual harm and the control failure. Depending on the circumstances, a supplier might reinstate responsibilities, reverse disciplinary action, correct records, retrain managers, or commission an independent review. Serious or repeated retaliation can justify escalated contract governance because it undermines the reliability of every future assurance statement. A hotline cannot function as a control if employees reasonably believe using it will damage their livelihood, reputation or prospects.

Serious Breach and Remediation

Whistleblowing failure should affect contract management when it reveals wider integrity, performance, or control problems, not merely an imperfect policy. A supplier that repeatedly suppresses reports, retaliates against reporters or conceals serious incidents may present continuing risk even after the original allegation is addressed. The response should be proportionate: corrective action and monitored improvement may be appropriate first, while persistent or grave misconduct can justify stronger contractual remedies or future procurement consequences.

The Procurement Act 2023 makes poor performance particularly significant for public authorities. Schedule 7 creates discretionary exclusion grounds for sufficiently serious contract breaches and for unsatisfactory performance where the supplier had a proper opportunity to improve but failed to do so. Updated government guidance explains that a sufficiently serious breach includes circumstances that lead to termination, damages, or settlement. In contrast, poor-performance mechanisms can include rectification or improvement plans before considering exclusion.

Since 1 January 2026, certain public-contract breaches and failures to improve must also be reported through contract performance notices, published within 30 days and capable of supporting discretionary exclusion for up to five years. Private-sector buyers have no equivalent statutory register, but nothing prevents comparable internal tracking through supplier scorecards, pre-qualification questionnaires and renewal decisions. A whistleblowing failure can therefore become procurement intelligence when it exposes material contractual non-performance or integrity risk.

Digital Whistleblowing Platforms

Digital whistleblowing platforms can widen access by allowing reports to be made remotely, outside working hours and without approaching line management. Good systems support encrypted submission, controlled case access, secure document handling and two-way anonymous communication through coded mailboxes or similar mechanisms. Technology helps because an anonymous reporter can answer follow-up questions without revealing their identity, reducing a principal investigative weakness of traditional anonymous letters or unmonitored email accounts.

The EU Whistleblower Directive provides a useful benchmark even where it does not govern

a UK organisation directly. Internal channels within scope must be designed securely to protect confidentiality and prevent unauthorised access, acknowledge receipt within seven days and ordinarily provide feedback within three months. It also permits third parties to operate reporting channels externally. These requirements demonstrate that a reporting platform is a governed process, not simply an online form.

Platform selection should examine hosting location, encryption, identity management, authentication, audit logging, administrator privileges, data export and deletion capability. A vendor may process allegations involving health, criminal conduct, trade-union membership or other sensitive information, making security and privacy architecture central to procurement. Buyers should establish where information is stored, who can decrypt it, how support personnel access cases and whether subcontractors participate in hosting, analytics, translation or case management.

Accessibility matters as much as technical security. Workers may lack corporate email, use shared devices, speak different languages, or have disabilities that affect how they communicate. A mobile-friendly platform can broaden participation, but an app requiring installation on an employer-managed device may deter reporting. Organisations should provide alternative channels, such as telephone or in-person reporting, so digital convenience does not become a barrier for people whose circumstances make the preferred technology unsafe.

Artificial Intelligence and Whistleblowing

Artificial intelligence can help identify relationships across large volumes of allegations, transactions and supplier data that human reviewers might miss. Natural-language tools can cluster recurring themes, detect references to the same supplier under different names and highlight links between reports and unusual payments. Used carefully, AI can help investigators prioritise review and identify systemic patterns, particularly where multinational organisations receive thousands of concerns across languages, business units and reporting channels.

The technology should support, not replace, judgement. Whistleblowing allegations are context-rich, often incomplete, and can have serious consequences for named individuals. Automated risk scoring can reproduce bias in historical case outcomes or treat unusual language as evidence of credibility. The UK Government's AI Playbook emphasises meaningful human control at appropriate stages and lifecycle governance, particularly where automated analysis may influence whether an allegation is investigated, escalated, or closed.

Public-sector transparency requirements are also developing. Central government departments and certain arm's-length bodies within the scope of the Algorithmic Transparency Recording Standard must document relevant algorithmic tools used in decision-making and make that information publicly accessible. A whistleblowing triage system that materially influences public-sector decisions may therefore raise transparency, explainability and governance questions alongside confidentiality concerns, especially if a supplier's proprietary model makes its reasoning difficult to scrutinise.

AI can also help protect investigators from information overload. Systems may summarise lengthy case histories, compare similar allegations or flag transactions matching known fraud typologies. The benefit is operational rather than evidential: investigators should not treat machine-generated conclusions as proof. Investigators must validate source material, preserve original records and record how automated assistance influenced decisions. A model can suggest where to look; accountable human decision-makers remain responsible for fair findings.

AI as a New Source of Risk

AI creates new whistleblowing risks because wrongdoing can be embedded in models, datasets and automated workflows that ordinary employees cannot easily inspect. Staff may

discover discriminatory outputs, unsafe recommendations, unauthorised surveillance, fabricated records or systems operating beyond approved purposes. When management has invested heavily in deployment, employees who challenge the system may face the same commercial pressure as traditional whistleblowers who question profitable products or important supplier relationships.

Procurement adds another layer because organisations may buy AI without the source code, training data, or technical capability to test it independently. The UK Government's AI Playbook instructs public bodies to involve commercial colleagues early and align responsible-use expectations between internally developed and third-party systems. Contracts can require transparency about model limitations, data sources, monitoring, change control and incident reporting rather than assuming a supplier's assurance automatically transfers to the customer.

Legal regimes are also evolving unevenly. The EU AI Act now applies certain governance and general-purpose AI obligations. At the same time, high-risk rules for areas including employment, education, critical infrastructure and migration are scheduled to apply from 2 December 2027 following the 2026 amendments. UK organisations operating internationally may therefore encounter regulatory duties different from domestic requirements, making employee reporting important where systems are deployed across jurisdictions under different classifications and controls.

Data Analytics as the Second Whistleblower

Data analytics can expose patterns no individual employee sees. Duplicate invoices, unusual payment timing, repeated threshold-level purchases, shared bank accounts, and supplier-director links may emerge only when datasets are compared across functions. In that sense, analytics behaves like a second whistleblower: it raises anomalies for investigation without alleging motive. The discipline is to treat the output as intelligence requiring context, not as automated proof that fraud or misconduct occurred.

The National Fraud Initiative demonstrates the scale of structured matching. Between April 2022 and March 2024, it identified or prevented £510.1 million of fraud, overpayments and errors across the UK. Trade-creditor and procurement matches produced £11 million of outcomes, including 819 duplicate payments totalling £11 million, of which £10.3 million was recovered. The programme shows how cross-dataset analysis can expose anomalies that ordinary transaction-by-transaction controls have missed.

Analytics can also identify conflicts. National Fraud Initiative procurement matching compares employee information with company data to identify people who may be directors of organisations trading with their employer or who may not have declared relevant financial interests. Such matches are leads, not findings: names can coincide, and legitimate disclosed relationships exist. Investigation should therefore verify identity, declaration status, influence over procurement and the commercial history before concluding misconduct.

Human disclosures make analytics stronger by providing hypotheses. A report that one manager repeatedly favours a supplier can prompt analysis of award concentration, pricing, variations and approval patterns; conversely, unexplained data anomalies can guide investigators towards people likely to understand the transactions. Combining both sources reduces dependence on chance. Employees see motives, conversations and behaviour, while data sees repetition, scale and relationships across periods or organisational boundaries that individuals may never encounter.

Governance is essential because analytics can create new risks. Poor-quality data, biased thresholds or unrecorded exceptions can generate false positives, while excessive surveillance can undermine trust. Organisations should define what analyses are proportionate, who may access results, how leads are validated and when records are deleted. The strongest model treats analytics as controlled assurance intelligence, separating anomaly detection from disciplinary judgment and allowing individuals to challenge conclusions reached from incomplete or misleading data.

Procurement Analytics

Procurement analytics can convert routine purchasing records into fraud and governance intelligence. Useful tests include duplicate invoice matching, spend just below approval thresholds, repeated retrospective orders, supplier concentration, unusual contract variations and payment to dormant or newly created vendors. Analysis can also compare supplier bank details, employee addresses or company directorships where lawful and proportionate. The objective is not constant suspicion but systematic identification of transactions that deserve closer human examination.

The National Fraud Initiative's 2022–24 results show what relatively simple matching can achieve. It identified 819 duplicate trade-creditor payments worth £11 million and recovered £10.3 million, while correcting or deleting a further 548 duplicate supplier-standing-data records. Luton Borough Council recovered a £34,000 duplicate payment involving similarly named creditors after an NFI match highlighted it. Basic data quality and matching therefore have direct financial value alongside fraud prevention.

Concentration analytics can reveal different risks. A supplier receiving an unusually high proportion of awards may be excellent, but the pattern becomes more significant when combined with repeated exceptions, limited competition or poor performance. Dashboards should therefore connect spend concentration with contract history, competition rates, conflict declarations and supplier performance. Statistical outliers are most informative when procurement professionals can explain whether commercial circumstances justify them or whether the pattern contradicts expected market behaviour.

Analytics should also test the purchasing process itself. Repeated purchase orders at £9,900 beneath a £10,000 approval threshold, invoices dated before requisitions or identical approvers across supplier setup and payment can indicate weak segregation or deliberate avoidance. Controls can flag combinations automatically, but investigators should preserve proportionality. A system designed to identify risk should not replace professional judgment about legitimate emergencies, framework call-offs, phased requirements, or other valid exceptions.

Protecting Whistleblower Data

Whistleblowing files can contain some of an organisation's most sensitive information: identities, allegations, health details, trade-union information, suspected criminal conduct, personal relationships and commercially confidential records. Protection therefore requires more than keeping the reporter's name secret. Organisations need a lawful basis for processing, data minimisation, appropriate access controls, secure storage and defensible retention arrangements, with additional conditions where special-category or criminal-offence data is processed under UK data-protection law.

Access should be limited by role, not seniority. Case investigators may need full evidence, while board members often require anonymised themes and outcomes rather than names or underlying documents. Technical administrators should not automatically gain unrestricted access to content merely because they support the platform. The ICO's own safeguards policy emphasises technical and organisational measures, secure processing, data-protection-by-design and access controls, illustrating the standard expected when sensitive investigative information is handled.

Retention needs similar discipline. The UK GDPR does not prescribe one universal retention period; ICO guidance on employee monitoring requires organisations not to retain personal information longer than necessary and to justify periods by purpose, business need and legal obligations. Whistleblowing records may need to survive litigation, regulatory enquiries or recurring investigations, but "keep everything forever" is not a defensible default. Retention schedules should differentiate allegations, evidence, case outcomes and anonymised trend data.

Security controls should anticipate that the subject of an allegation may hold organisational power. If an accused executive can access the case-management system, email archive or identity-management console, nominal confidentiality may fail. Privileged access should therefore be tightly restricted, logged and periodically reviewed. The NCSC advises that privileged users receive only necessary access and that security events are logged and monitored, principles directly applicable to digital whistleblowing systems holding highly sensitive investigative records.

External platform providers create processor and transfer considerations. Contracts should address security, confidentiality, breach notification, subprocessors, deletion, export and support access. If organisations transfer personal information internationally, they must assess whether UK restrictions on international transfers apply and use appropriate safeguards where required. ICO guidance updated in January 2026 describes the current international-transfer framework and the data-protection test used to assess certain restricted transfers effectively.

Protection also requires disciplined communication. Investigators should avoid copying allegations unnecessarily, forwarding reports through ordinary email chains or reproducing identifying details in board papers. Witnesses and accused persons may require enough information for fairness, but disclosure should be purposeful and proportionate. A technically secure platform cannot compensate for investigators casually revealing the reporter through conversation, document naming, distinctive quotations or unnecessarily detailed summaries that make identity obvious to colleagues.

Can Technology Identify an Anonymous Reporter Accidentally?

Metadata and contextual clues can unintentionally undermine anonymous reporting. IP addresses, device identifiers, login credentials, document properties, timestamps, location data or distinctive writing patterns may narrow the pool of possible reporters even when a platform does not request a name. Organisations promising anonymity should therefore understand what technical information their systems and vendors collect and whether administrators, investigators or security tools can access information capable of revealing identity.

The distinction between anonymous and pseudonymous information is legally important. ICO guidance explains that information remains personal data where an individual can be re-identified using reasonably available means, even if direct identifiers have been removed. Pseudonymisation can reduce risk but does not take information outside UK GDPR. A case labelled “anonymous” should therefore not be treated as genuinely anonymous if platform logs or organisational context still allow identification of the reporter.

Behavioural information can also defeat anonymity without any technical tracing. A report may refer to a meeting attended by three people, quote an unpublished email or describe an event witnessed by only one employee. Investigators should avoid unnecessary efforts to infer identity and should warn reporters honestly that anonymity cannot always be guaranteed. The objective is to minimise avoidable identification while preserving enough information to investigate fairly and protect others involved.

Different Legal Regimes

Multinational whistleblowing systems operate across materially different legal frameworks. In Great Britain, protection principally arises through the Employment Rights Act 1996, as amended by the Public Interest Disclosure Act 1998, and depends on matters including worker status, qualifying subject matter, reasonable belief and the route of disclosure. Acas guidance confirms that several categories, including genuinely self-employed people and some volunteers, generally fall outside statutory protection even if an organisation chooses to receive their concerns.

The European Union follows a different model under Directive 2019/1937, implemented

through national laws that differ across Member States. The Directive generally requires private legal entities with at least 50 workers to establish internal reporting channels, protects confidentiality and prescribes procedural features such as seven-day acknowledgement and feedback normally within three months. It also protects broader work-related categories in specified circumstances, making a single UK-designed policy insufficient for EU operations.

National implementation still matters. A multinational cannot assume that complying with the Directive's baseline in one Member State automatically satisfies another's employment, data-protection, works-council or procedural requirements. Local laws may differ on anonymous reporting, investigation responsibility, permitted subject matter and sanctions. Global platforms should therefore be configured around a common minimum standard while allowing jurisdiction-specific routes, notices, deadlines and escalation arrangements where local legislation requires them.

Regulatory scope can differ, as can employment protections. Financial services, healthcare, competition, environmental and public-procurement regimes may provide prescribed or specialist reporting channels unavailable in another jurisdiction. Employees should be told which external authorities are relevant, rather than directed to a single corporate hotline. A global policy that discourages lawful external reporting can create legal and cultural risk, particularly where local legislation expressly protects direct disclosure to competent regulators.

Organisations should therefore map legal requirements before centralising investigations. The map should cover who qualifies for protection, reportable subject matter, anonymity, confidentiality, response deadlines, employee-representation requirements, record retention and cross-border data transfers. Corporate principles can remain consistent—trust, impartiality, protection and proper follow-up mirror ISO 37002—but the legal mechanism for delivering those principles must reflect the country in which the reporter, employer and alleged wrongdoing are located.

Cultural Differences

Whistleblowing culture cannot be exported simply by translating a policy. In some workplaces, employees are comfortable challenging management directly; in others, hierarchy, age, status or expectations of loyalty make such behaviour socially difficult even where legal protection exists. A global organisation may therefore see radically different reporting rates between countries without equivalent differences in misconduct. Low usage should prompt investigation of accessibility, trust and local perceptions rather than automatic conclusions about ethical performance.

Language itself can affect meaning. Terms equivalent to “whistleblower” may carry associations with informing, betrayal or political denunciation, making employees reluctant to identify with the label. Organisations can use locally tested language around speaking up, integrity or raising concerns while retaining legal accuracy in formal notices. Training should also use realistic local scenarios rather than importing headquarters examples that employees do not recognise as relevant to their working relationships or social context.

Management behaviour matters particularly in high-power-distance cultures. A policy encouraging reports means little if local leaders visibly punish disagreement, expect problems to be resolved through hierarchy or equate external escalation with disloyalty. Independent channels, local ethics advisers and confidential third-party reporting can provide alternatives, but only repeated fair treatment establishes credibility. Global leaders should examine retaliation allegations, employee surveys and case outcomes by location rather than assuming policy publication creates equivalent psychological safety.

Cultural adaptation must not become ethical relativism. Organisations should not tolerate bribery, forced labour, serious safety breaches, or falsification because local practice treats them as normal. The challenge is to deliver consistent standards through methods that people can realistically use. ISO 37002 is expressly designed for organisations of different sizes,

sectors, and jurisdictions, providing stable principles of trust, impartiality, and protection. In contrast, communication, channel design, and investigation practices adapt locally.

Whistleblowing and the Global Supply Chain

Global supply chains separate buyers from the people who often possess the clearest evidence of wrongdoing. Workers may be employed by subcontractors, labour agencies, factories, logistics providers or raw-material producers several contractual layers away. A corporate hotline designed only for direct employees therefore leaves major assurance gaps. Reporting architecture should follow material risk through the chain, particularly where labour exploitation, corruption, product safety, environmental harm or cyber dependency sits below Tier One.

Accessibility becomes harder as distance increases. Workers may lack corporate devices, reliable internet, literacy in the buyer's language or confidence that a foreign hotline is genuinely independent. Reporting routes may therefore need local telephone numbers, multilingual web access, trusted worker representatives or civil-society partners. The channel should explain confidentiality, permissible anonymity and what the buyer can realistically do, avoiding promises of protection or investigation powers that do not exist in the worker's jurisdiction.

The EU Whistleblower Directive recognises that people outside conventional employment can possess relevant information, covering specified categories connected through work-related activities and allowing channels to be made available beyond an entity's own workers. Its recitals specifically contemplate service providers, distributors, suppliers and business partners receiving information about reporting procedures. That principle is valuable globally: serious risk does not respect corporate boundaries, so assurance channels should not stop automatically at the customer's payroll.

Modern-slavery guidance provides a practical supply-chain model. The Home Office recommends multiple routes for workers, including those in supply chains, to report concerns anonymously and in languages they understand. PPN 009 similarly promotes grievance mechanisms, worker engagement, supply-chain mapping and contractual controls. These measures acknowledge that direct supplier management reports can never provide complete visibility into labour conditions several tiers below the purchasing organisation.

Global channels also need triage that can identify jurisdiction. A bribery allegation in one country, a forced-labour concern in another, and a cyber incident affecting several regions may trigger different legal, regulatory, and reporting obligations. Centralisation can improve consistency, but local counsel, safeguarding expertise or specialist regulators may still be necessary. Case systems should therefore capture location, employing entity, supplier tier and affected operations early without collecting unnecessary personal information merely because the platform permits it.

The objective is credible reach, not theoretical availability. A hotline technically open worldwide provides little assurance if workers do not know it exists, cannot use their language or reasonably expect retaliation. Buyers should test awareness through interviews, surveys and audits, then compare usage with risk indicators. Global supply-chain whistleblowing succeeds when people closest to the risk can communicate safely with decision-makers who can act on what they report.

Workers Where Legal Protection Is Weak

Contractual protection becomes especially important where local whistleblowing law is narrow, remedies are slow or particular categories of workers fall outside statutory coverage. A buyer can require non-retaliation, confidential reporting, investigation cooperation and remediation from suppliers, creating commercial consequences where workers are mistreated. Those commitments can materially improve behaviour, but they do not transform the worker's legal status or create tribunal, court or regulatory remedies that domestic legislation does not

provide.

Great Britain itself illustrates the limitation. Acas states that genuinely self-employed people, volunteers without enforceable employment contracts, non-executive directors and some other categories are generally outside statutory whistleblowing protection. However, organisational policies may still allow them to report. A multinational supplier code can therefore extend access more broadly than the law, but it should distinguish voluntary organisational protection from legally enforceable whistleblower rights so that reporters are not given false confidence.

Meaningful protection requires leverage after the report. Buyers may insist on investigation safeguards, monitor retaliation indicators, require corrective action and escalate repeated mistreatment through contract governance. In severe cases, they may consider suspension, remediation plans or responsible disengagement. The strongest approach also signposts independent unions, regulators, NGOs or legal advice where available, recognising that contractual influence is one protective layer rather than a replacement for functioning national institutions.

Cross-Border Investigations

Cross-border investigations are difficult because a single case can engage employment, privacy, secrecy, blocking, surveillance, and evidence rules in several jurisdictions. A central investigation team may wish to export emails, witness statements or hotline records to the UK. Yet, lawful collection in the source country does not automatically make onward transfer lawful. Planning should establish where data originates, which entity controls it, where investigators sit and what legal mechanisms govern each transfer.

UK data-protection rules remain relevant when personal information is transferred internationally from the UK. ICO guidance updated in January 2026 sets out a three-step approach to identifying restricted transfers. It explains the safeguards available under UK GDPR, including the International Data Transfer Agreement, Addendum and binding corporate rules. Where required, organisations must also consider the statutory data-protection test before relying on certain transfer mechanisms rather than assuming group-company sharing is automatically permitted.

Employment law can complicate interviews and evidence gathering. Local rules may require works-council involvement, restrict monitoring, protect certain communications, or impose procedures before collecting disciplinary material. Investigators should therefore avoid importing UK practice wholesale. A process that is proportionate and lawful in London may breach local requirements elsewhere, undermining both employee rights and evidence reliability. Early jurisdictional mapping reduces the risk of discovering these constraints after sensitive evidence has already crossed borders.

Evidence integrity also becomes harder when multiple providers handle information. Translation, e-discovery, forensic imaging and external counsel can each create new copies, access rights and transfer points. Case management should record provenance, collection method, custodianship and material changes so investigators can explain where evidence came from and how it was preserved. A multinational inquiry must remain able to distinguish source material from translations, summaries, automated extractions, and investigator annotations.

Confidentiality requires realistic communication with reporters. Identity may need to be shared with local counsel, regulators or courts, and absolute anonymity may be impossible where facts identify the source. Investigators should explain these limits before unnecessary disclosure occurs and minimise cross-border circulation of identifying data. The safest principle is purpose limitation: move only what is genuinely required for investigation, legal compliance or remediation rather than replicating complete case files across every participating jurisdiction.

Global Standards with Local Delivery

Global organisations need common principles so that a concern is not treated seriously in one country and casually in another. ISO 37002 offers a useful framework built around trust, impartiality and protection, covering receipt, assessment, handling and closure of reports. The standard was reviewed and confirmed as current in 2026. It is intentionally adaptable across different organisational sizes, sectors and jurisdictions, making it suitable as a governance baseline rather than a substitute for local law.

Consistency should apply to core expectations: accessible reporting, confidentiality, protection from retaliation, impartial triage, competent investigation, documentation and remediation. Delivery can then vary appropriately. One country may favour telephone reporting, another works-council channels and another encrypted web platforms. Response deadlines may also differ. A global policy is strongest when it states minimum principles clearly while local appendices explain the lawful processes, authorities and employment protections applicable to each operating environment.

Local adaptation should be governed, not improvised. Country teams should not be allowed to weaken confidentiality or independence simply because hierarchical practices make those controls uncomfortable. Equally, headquarters should not insist on procedures that conflict with local law or make channels culturally unusable. Document exceptions, have them legally reviewed, and approve them through central governance to create visibility into where the global standard cannot be delivered exactly and what compensating safeguards are used.

Interpret metrics locally as well as globally. Comparing raw report volumes across countries can mislead because workforce size, legal awareness, language, channel availability and cultural attitudes differ. More useful measures include reporting awareness, investigation timeliness, retaliation allegations, repeat themes and confidence in speaking up. Central boards can then identify locations where unusually low usage coincides with high operational risk, poor survey results or repeated external complaints and commission targeted assurance.

Procurement Professionals as Both Gatekeepers and Whistleblowers

Procurement professionals occupy an unusual position because they are both control owners and potential witnesses. They design competitions, protect confidential information, challenge conflicts, negotiate contracts and monitor supplier performance, yet those responsibilities can expose them to pressure from executives, operational teams and strategically important suppliers. When ordinary professional challenge is overridden, the buyer who normally enforces governance may become the person who needs protection from the governance hierarchy itself.

The UK Government Supplier Code of Conduct recognises reciprocal challenge. It expects suppliers to speak out when officials, civil servants, or other suppliers fail to uphold expected values, and when projects or services are unlikely to succeed because of government behaviour or poor governance. That principle should work internally as well. Procurement professionals need permission to say that a preferred route is non-compliant, a business case is misleading, or a supplier relationship has become unsafe.

Professional independence becomes difficult when procurement is measured principally by speed and savings. A buyer who delays an award to investigate a conflict may be portrayed as obstructive, while one who challenges an executive-sponsored supplier may fear career consequences. Performance frameworks should therefore recognise integrity, competition, documentation and risk management alongside delivery. Organisations create perverse incentives when procurement employees are rewarded for completing transactions quickly but personally absorb the consequences of stopping questionable ones.

Whistleblowing should remain a last-resort escalation route rather than the normal mechanism for procurement disagreement. Many disputes about specification, value, procedure or risk belong within ordinary professional governance. The distinction arises when an employee

reasonably believes wrongdoing or serious risk is being concealed, tolerated or imposed through authority. Clear escalation criteria help prevent routine challenge from being labelled whistleblowing while ensuring genuine concerns are not dismissed as mere commercial disagreement.

Boards should recognise procurement staff as part of the organisation's early-warning network. Their access to suppliers, pricing, conflicts, contract changes and performance data gives them visibility across organisational boundaries that many functions lack. Training should therefore cover both how to receive supplier concerns and how to raise their own. Procurement cannot credibly demand ethical behaviour from the supply market if its own professionals lack safe routes to challenge internal misconduct.

Create Escalation Routes Outside the Procurement Hierarchy

An escalation route confined to procurement management fails when procurement leadership is implicated in the concern. A category manager alleging manipulation by the procurement director cannot reasonably be expected to report solely through that director's chain. Policies should therefore provide direct access to compliance, internal audit, legal counsel, an audit committee chair, a senior independent director or an appropriately governed external channel, depending on organisational structure and the seriousness of the allegation.

Independence requires more than a different email address. The alternative recipient must possess authority to preserve records, prevent interference, commission investigation and escalate findings without permission from the person implicated. Case access should also be separated technically where necessary. If senior procurement leaders administer the reporting system or can automatically view every allegation, the formal existence of an alternative route does not provide meaningful independence for employees considering whether to use it.

The same principle should cover suppliers. A vendor alleging that procurement personnel demanded favours, leaked competitor information or manipulated an evaluation needs a route outside the commercial relationship owner. The Government Supplier Code expressly expects suppliers to speak out when government personnel or other suppliers do not uphold required standards. Organisations should make that expectation credible by publishing an independent recipient rather than forcing the supplier to complain to the buyer controlling its contract.

Build Whistleblowing into Supplier Governance

Whistleblowing is most effective when incorporated throughout supplier governance rather than added after a crisis. Pre-contract due diligence can examine reporting arrangements and retaliation controls; onboarding can communicate customer expectations and escalation routes; contract reviews can consider material themes; supplier codes can establish behavioural standards; and contracts can address notification, audit and remediation. The result is a continuous assurance model connecting worker intelligence with commercial governance from selection through exit.

The Government Supplier Code of Conduct already treats whistleblowing as a supplier-governance expectation, requiring comprehensive policies that permit anonymous, safe reporting without repercussion. PPN 009 adds practical modern-slavery mechanisms including worker grievance routes, supply-chain mapping, subcontractor controls and remedial action. NCSC guidance similarly recommends ongoing supplier-security monitoring rather than relying upon one-off assessment. Together these frameworks show that speak-up information belongs alongside performance, risk and assurance throughout contract management.

Onboarding is particularly important because expectations are easiest to establish before problems arise. Suppliers should know what must be reported, which channels workers can use, how confidentiality will be handled and which obligations extend to subcontractors. Buyers should also understand the supplier's existing mechanisms rather than automatically duplicating them. Where a credible independent system already exists, integration and

escalation arrangements may provide better assurance than imposing another hotline workers neither recognise nor trust.

Periodic reviews should examine effectiveness rather than policy existence. Questions can cover report awareness, case volumes, serious themes, investigation times, retaliation allegations, regulatory referrals and corrective actions, with personal information shared only where necessary. The objective is to detect whether risk is changing, not to obtain unrestricted access to employee case files. High-risk findings should connect to supplier improvement plans, audit activity, contract performance and enterprise risk reporting.

At contract exit, whistleblowing obligations should not disappear before unresolved concerns are addressed. Records may need retention, investigations may continue, and reporters may remain vulnerable after services transfer. Exit plans should allocate responsibility for open cases, evidence preservation and continuing cooperation. Supplier governance reaches maturity when speaking up is treated not as a compliance appendix or an HR matter, but as a source of commercial intelligence that influences selection, monitoring, remediation, and future procurement decisions.

Protect Procurement Integrity

Speaking up protects more than the individual transaction being questioned. Procurement integrity supports competition, value, public confidence and the defensibility of organisational decisions. Under section 12 of the Procurement Act 2023, contracting authorities carrying out covered procurement must have regard to value for money, public benefit, information sharing and acting, and being seen to act, with integrity. They must also treat suppliers equally unless relevant differences justify different treatment.

Procurement staff are often the first to see conduct that threatens those objectives: unexplained specification changes, selective information, conflicts, suspicious bids, repeated exceptions or attempts to override evaluation. Speaking up about such behaviour protects organisational funds before the problem becomes an external challenge. It also protects innocent suppliers because fair escalation can identify whether an anomaly has a legitimate explanation rather than allowing suspicion to circulate informally without evidence or due process.

Integrity also has a reputational dimension. Government guidance emphasises that contracting authorities must consider not only whether they act with integrity but whether the procurement can reasonably be seen as proper. That matters because unsuccessful bidders and the public rarely possess every internal fact. Clear records, consistent treatment and safe internal challenge allow organisations to demonstrate that decisions resulted from defensible commercial judgement rather than undisclosed influence or predetermined preference.

Where misconduct is established, the consequences can extend into supplier eligibility. Updated 2026 guidance under the Procurement Act explains that exclusion grounds address risks involving effective competition, supplier integrity, public funds and reliable delivery. Serious breach, poor performance, competition concerns and improper procurement behaviour can therefore affect participation in future public contracts. Protecting procurement integrity is consequently part of market stewardship as well as immediate contract governance.

The Buyer's Responsibility Does Not End at Tier One

A buyer can outsource activity but not all responsibility for understanding material supply-chain risk. Tier One suppliers may rely on subcontractors, labour agencies, manufacturers, technology providers and raw-material sources that sit several contractual layers away. The customer's practical influence may diminish with distance, but the consequences can still return through modern slavery, safety failures, cyber incidents, environmental harm or product defects. Assurance must therefore follow significant risk beyond the immediate invoice issuer.

The practical challenge is proportionality. Buyers cannot map every low-risk purchase to raw-

material origin or run direct hotlines for every worker globally. They can, however, identify categories where labour intensity, geography, criticality, safety, or subcontracting create elevated risk and require deeper visibility. Risk-based mapping, pass-through clauses, worker access and independent audits allow resources to follow exposure rather than treating every supplier relationship as equally opaque or equally significant.

Whistleblowing extends that visibility because lower-tier workers can reveal what contractual diagrams omit. A subcontractor employee may identify an undeclared labour broker, an unauthorised production site, or a concealed safety problem that the Tier One supplier has not reported. The buyer should not casually bypass supplier governance, but serious intelligence from deeper tiers should reach someone with the authority to investigate, protect affected workers, and require remediation throughout the chain.

Speaking Up or Staying Silent?

The central choice is rarely as simple as courage versus cowardice. People decide whether to speak by assessing consequences: whether leaders listen, identities remain protected, investigations are fair and previous reporters were treated well. Law can influence that calculation, but organisational behaviour often determines it. A technically compliant whistleblowing policy will not overcome a culture in which inconvenient information damages careers, while a trustworthy system can make difficult disclosures feel like ordinary professional responsibility.

Great Britain's legal framework provides meaningful protection when statutory conditions are met. Acas explains that qualifying whistleblowers can be protected from detriment and, for employees, automatic unfair dismissal, with protection beginning from the start of employment. Yet coverage is not universal: genuinely self-employed people, some volunteers, non-executive directors and members of the armed forces are generally outside ordinary statutory protection. Organisational systems therefore remain important even where legislation provides no complete safety net.

Hierarchy also shapes the decision. A junior buyer considering whether to challenge an executive-sponsored supplier may weigh promotion prospects, reputation and collegial relationships against an uncertain organisational response. A subcontractor worker may fear losing wages or accommodation. A cybersecurity engineer may fear being blamed for delaying launch. Each person experiences the same governance question differently: does the organisation genuinely want to know what they know, even when the answer is commercially inconvenient?

Current reporting volumes show that people will use channels when they believe doing so has value. The FCA assessed 1,375 reports in 2025–26, 22% more than the previous year, while Freedom to Speak Up Guardians recorded 37,770 NHS cases during 2025–26. High numbers do not automatically prove healthy cultures, but they show that substantial organisations can receive large volumes of concerns without treating reporting itself as organisational failure.

The opposite is equally important. Silence can result from low misconduct, but it can also reflect fear, futility or lack of awareness. Boards therefore need more than case counts. They should examine employee surveys, retaliation allegations, exit interviews, audit findings, supplier complaints and external regulatory contact. The question is not whether whistleblowing numbers are low; it is whether people who encounter wrongdoing believe there is a safe and worthwhile route through which to challenge it.

Across procurement and supply chains, that judgement has consequences beyond employment relations. Speaking up can expose bribery, bid-rigging, false invoicing, modern slavery, product defects, cyber weaknesses and environmental misconduct before intervention occurs. Staying silent lets weak signals remain isolated until losses or harm connect them publicly. The organisational objective should therefore be to reduce the personal cost of reporting so that the commercially rational action for the individual is also the ethically responsible one.

Can Legislation Create Courage?

Legislation can change incentives by prohibiting retaliation and providing remedies, but it cannot manufacture confidence in an organisation. In Great Britain, whistleblowing protection operates mainly through the Employment Rights Act 1996, as amended by the Public Interest Disclosure Act 1998. Acas states that protected workers may claim detriment and employees may claim automatic unfair dismissal where the legal tests are satisfied. Those rights matter because they create consequences when organisations punish legitimate disclosure.

The limits are equally important. Employment tribunal claims are normally subject to a three-month-minus-one-day time limit, and applications for interim relief following alleged whistleblowing dismissal must ordinarily be made within seven days of termination. Legal protection therefore often operates after relationships have already deteriorated. A successful claim can provide remedy, but it cannot restore every lost opportunity, repair every damaged professional relationship or erase the stress created by retaliation.

Legislation also depends on eligibility and disclosure route. ACAS notes that qualifying disclosures require reasonable belief that relevant wrongdoing has occurred and that the disclosure is in the public interest. Protection varies according to whom the person tells, while some categories of people fall outside ordinary statutory coverage. A policy promising simply that “whistleblowers are protected by law” can therefore be misleading unless employees understand that legal protection has defined conditions and boundaries.

Can Governance Reduce the Need for Courage?

Good governance cannot eliminate anxiety, but it can reduce the amount of personal bravery required to report concerns. Clear routes, confidential handling, independent escalation and visible non-retaliation change the perceived risk of speaking. When employees know what will happen after a report and have seen concerns investigated fairly, disclosure becomes part of the control system rather than an exceptional confrontation with authority. Predictability is one of the strongest forms of psychological protection.

Boards should therefore judge speak-up arrangements by behaviour, not publication. Relevant questions include whether employees know the channels, whether cases are acknowledged quickly, whether conflicts are removed from investigations and whether reporters experience detriment. Freedom to Speak Up data for 2025–26 recorded more than 1,100 NHS cases in which workers reported experiencing detriment after speaking up. Even within an established national framework, protection remains an ongoing operational challenge rather than a solved policy issue.

Governance can also distribute responsibility so that the reporter is not carrying the whole burden. Once credible information is raised, management should preserve evidence, assess immediate risks, appoint independent investigators and decide whether regulators or law enforcement need notification. The employee should not have to collect more evidence, confront suspected wrongdoers, or repeatedly persuade multiple layers of management. A mature system shifts responsibility from individual courage to the organisation’s formal processes.

External oversight provides another layer. Prescribed persons, regulators, audit committees and independent directors create alternative routes when ordinary management channels are conflicted. The FCA’s 2025–26 data shows how whistleblower information can become regulatory intelligence and direct action. Credible external escalation also disciplines internal governance because organisations know that concerns suppressed internally may eventually reach authorities with powers to compel information, investigate, and sanction misconduct.

Contract design can extend the same principle into supply chains. Buyers can require grievance mechanisms, confidential reporting, non-retaliation and notification of serious concerns, while PPN 009 supports worker-facing mechanisms and remedial action in higher-risk government supply chains. These measures do not guarantee courage, particularly where

employment insecurity is severe, but they reduce the dependence on extraordinary individuals willing to sacrifice their position to make organisational risk visible.

When Commercial Success Conflicts with Speaking Up

The hardest whistleblowing cases arise when the information threatens something the organisation values: a profitable contract, strategic supplier, important customer, product launch or executive reputation. When the commercial consequence of disclosure is obvious, decision-makers can begin rationalising delay as proportionality, further investigation or relationship management. The real governance test is whether inconvenient information receives the same evidential seriousness when acting upon it may reduce revenue, increase cost or disrupt operational plans.

Carillion illustrates why commercial importance should sharpen scepticism rather than weaken it. Its 420 public-sector contracts embedded the business deeply across essential services before liquidation. Dependency made failure consequential, but dependency could not make the underlying financial position sound. Organisations should therefore avoid confusing the difficulty of replacing a supplier with evidence that concerns about that supplier are less credible. Operational resilience exists partly so uncomfortable facts can be acted upon without catastrophic dependence.

Commercial pressure can influence smaller decisions long before a crisis. A contract manager may hesitate to record poor performance before renewal; a buyer may avoid reporting a conflict because competition is already delayed; a quality engineer may suppress a non-conformity to protect shipment. Strong governance anticipates these moments by separating assurance from delivery incentives and ensuring that people who stop or challenge activity are not judged solely by immediate commercial disruption.

The Cost of Ignoring the Messenger

Ignoring a credible messenger rarely makes the underlying risk disappear. It removes one opportunity to discover the problem while it is still comparatively contained. The eventual cost may take the form of fraud losses, remediation, litigation, regulatory penalties, service interruption or management time. More difficult to quantify are lost trust, damaged careers and the institutional memory created when employees learn that raising inconvenient information is personally dangerous and operationally pointless.

The Horizon scandal provides the clearest contemporary financial illustration. Government data shows approximately £1.697 billion had been paid in financial redress by 28 August 2026. The statutory inquiry has examined governance, oversight and whistleblowing alongside technical and contractual issues. Redress is not itself a measure of the cost of ignored whistleblowers, but its scale demonstrates how unresolved organisational failures can create liabilities that continue for years after the original decisions were taken.

The cost of ignoring a reporter is also cultural. Employees watch what happens to colleagues who challenge wrongdoing and adjust their future behaviour accordingly. One mishandled disclosure can suppress information far beyond the original case because other employees infer that silence is safer. The financial impact of the next undisclosed fraud or safety failure may never be attributed to that cultural moment. Yet, the causal link can be as important as any failed technical control.

Boards should therefore consider whistleblowing failures as indicators of control effectiveness, not solely employee-relations incidents. A retaliation allegation, repeated unresolved disclosure or unexplained case closure should prompt questions about risk governance and management incentives. The cheapest concern to investigate is often the one raised before external damage occurs. Once regulators, courts, customers or journalists discover the same issue independently, the organisation loses both the opportunity for early correction and control over the narrative.

Summary – Silence Is a Governance Decision Too

Whistleblowing should not depend upon exceptional individuals willing to sacrifice careers to correct organisational failure. Boards, procurement teams and supply-chain leaders control whether reporting is accessible, whether investigations are independent and whether retaliation is tolerated. Every decision about channel design, confidentiality, supplier contracts, audit rights and escalation determines how difficult speaking up becomes. Silence may therefore reflect not employee indifference, but governance arrangements that make disclosure personally costly or apparently futile.

The scale of UK procurement expenditure makes that responsibility commercially significant, spanning central government, local authorities, the NHS, social housing and countless private contracts. Across such expenditure, wrongdoing can arise through bribery, conflicts, bid-rigging, invoice fraud, labour exploitation, unsafe products, environmental misconduct or cyber weakness. Procurement professionals operate where money, market information and supplier relationships intersect, making their ability to challenge behaviour a core component of organisational control rather than an optional ethical safeguard.

Effective governance combines human intelligence with other forms of assurance. Whistleblowing reports should be compared with spend analytics, audit findings, supplier KPIs, complaints, safety information and regulatory intelligence. The FCA's 2025–26 experience demonstrates the principle: 1,375 whistleblowing reports generated 4,375 allegations and contributed to 523 instances of direct action. Information becomes valuable when systems can connect it to evidence, risk assessment, and proportionate intervention.

Supply-chain responsibility also cannot stop at Tier One. Government modern-slavery guidance now explicitly addresses grievance mechanisms for supply-chain workers, subcontractor controls, mapping, direct worker engagement and remedial action. Similar logic applies to product, environmental and cyber risks. The people closest to an unsafe factory, compromised system or abusive labour practice may work several contracts away from the customer. Assurance architecture should give material intelligence a route back through those commercial layers.

Law can prohibit retaliation and provide remedies; governance can make those remedies less necessary. The strongest speak-up environment is one in which raising concern is routine, evidence is tested fairly, and management expects challenge. Organisations ultimately choose whether to treat uncomfortable information as disruption or intelligence. When silence is rewarded, and challenge penalised, staying silent is not merely an individual decision—it becomes an outcome the governance system has helped to produce.

Further Reading

The following primary sources, regulatory publications and inquiry reports informed the research and figures used throughout, and are recommended for readers wishing to explore particular themes in greater depth.

Legislation

- *Employment Rights Act 1996, Part IVA, as inserted by the Public Interest Disclosure Act 1998 (legislation.gov.uk)*
- *Modern Slavery Act 2015, section 54 (legislation.gov.uk)*
- *Bribery Act 2010 and Fraud Act 2006 (legislation.gov.uk)*
- *Procurement Act 2023 and accompanying statutory guidance (gov.uk)*
- *Economic Crime and Corporate Transparency Act 2023, failure-to-prevent-fraud offence (legislation.gov.uk)*
- *Digital Markets, Competition and Consumers Act 2024 (legislation.gov.uk)*

Government and Regulatory Guidance

- *Cabinet Office, Procurement Policy Note 009 – Tackling Modern Slavery in Government Supply Chains (gov.uk)*

- *Cabinet Office, UK Government Supplier Code of Conduct (gov.uk)*
- *Home Office, Modern Slavery: Statutory Guidance for England and Wales (gov.uk)*
- *Financial Reporting Council, UK Corporate Governance Code 2024 (frc.org.uk)*
- *Financial Conduct Authority, whistleblowing data and annual reports (fca.org.uk)*
- *Serious Fraud Office, annual reports and deferred prosecution agreements (sfo.gov.uk)*
- *Acas, whistleblowing guidance for employers and workers (acas.org.uk)*
- *Health and Safety Executive, health and safety statistics (hse.gov.uk)*
- *Office for Product Safety and Standards, Product Safety Database reports (gov.uk)*
- *Environment Agency, waste crime report (gov.uk)*
- *National Cyber Security Centre, supply chain security guidance (ncsc.gov.uk)*
- *Department for Science, Innovation and Technology, Cyber Security Breaches Survey (gov.uk)*
- *Information Commissioner's Office, guidance on personal data breaches (ico.org.uk)*
- *Gangmasters and Labour Abuse Authority, exploitation indicators (gla.gov.uk)*
- *Competition and Markets Authority, case decisions and green claims guidance (gov.uk)*
- *Advertising Standards Authority, adjudications (asa.org.uk)*
- *Regulator of Social Housing, whistleblowing and disclosures data (gov.uk)*
- *National Guardian's Office, NHS Freedom to Speak Up annual data (nationalguardian.org.uk)*
- *Ofgem, Renewables Obligation reporting and Drax investigation outcome (ofgem.gov.uk)*

Inquiries and Official Reports

- *Grenfell Tower Inquiry, Phase 2 Report (grenfelltowerinquiry.org.uk)*
- *Post Office Horizon IT Inquiry (postofficehorizoninquiry.org.uk)*
- *National Audit Office, reports on electronic-monitoring contracts and departmental assurance (nao.org.uk)*
- *House of Commons Work and Pensions and BEIS Committees, joint inquiry into the collapse of Carillion (parliament.uk)*

Other Sources

- *International Labour Organisation, global estimates of modern slavery and child labour (ilo.org)*
- *Cabinet Office, Civil Service People Survey (gov.uk)*
- *Intellectual Property Office, counterfeiting research (gov.uk)*